

WHOIS DATABASE: PRIVACY AND INTELLECTUAL PROPERTY ISSUES

HEARING BEFORE THE SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY OF THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES ONE HUNDRED SEVENTH CONGRESS FIRST SESSION

JULY 12, 2001

Serial No. 23

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

U.S. GOVERNMENT PRINTING OFFICE

73-612 PS

WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512-1800 Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
STEVE CHABOT, Ohio	MELVIN L. WATT, North Carolina
BOB BARR, Georgia	ZOE LOFGREN, California
WILLIAM L. JENKINS, Tennessee	SHEILA JACKSON LEE, Texas
ASA HUTCHINSON, Arkansas	MAXINE WATERS, California
CHRIS CANNON, Utah	MARTIN T. MEEHAN, Massachusetts
LINDSEY O. GRAHAM, South Carolina	WILLIAM D. DELAHUNT, Massachusetts
SPENCER BACHUS, Alabama	ROBERT WEXLER, Florida
JOE SCARBOROUGH, Florida	TAMMY BALDWIN, Wisconsin
JOHN N. HOSTETTLER, Indiana	ANTHONY D. WEINER, New York
MARK GREEN, Wisconsin	ADAM B. SCHIFF, California
RIC KELLER, Florida	
DARRELL E. ISSA, California	
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	

PHILIP G. KIKO, *Chief of Staff-General Counsel*

JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

HOWARD COBLE, North Carolina, *Chairman*

HENRY J. HYDE, Illinois	HOWARD L. BERMAN, California
ELTON GALLEGLY, California	JOHN CONYERS, JR., Michigan
BOB GOODLATTE, Virginia, <i>Vice Chair</i>	RICK BOUCHER, Virginia
WILLIAM L. JENKINS, Tennessee	ZOE LOFGREN, California
ASA HURCHINSON, Arkansas	WILLIAM D. DELAHUNT, Massachusetts
CHRIS CANNON, Utah	ROBERT WEXLER, Florida
LINDSEY O. GRAHAM, South Carolina	MAXINE WATERS, California
SPENCER BACHUS, Alabama	MARTIN T. MEEHAN, Massachusetts
JOE SCARBOROUGH, Florida	TAMMY BALDWIN, Wisconsin
JOHN N. HOSTETTLER, Indiana	ANTHONY D. WEINER, New York
RIC KELLER, Florida	

BLAINE MERRITT, *Chief Counsel*

DEBRA ROSE, *Counsel*

CHRIS J. KATOPIS, *Counsel*

ALEC FRENCH, *Minority Counsel*

CONTENTS

JULY 12, 2001

OPENING STATEMENT

The Honorable Howard Coble, a Representative in Congress From the State of North Carolina, and Chairman, Subcommittee on Courts, the Internet, and Intellectual Property	1
The Honorable Howard Berman, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Courts, the Internet, and Intellectual Property	2

WITNESSES

Mr. Stevan D. Mitchell, Vice President, Intellectual Property Policy, Interactive Digital Software Association (IDSA)	
Oral Testimony	5
Prepared Statement	6
Mr. Timothy Trainer, President, International Anticounterfeiting Coalition (IACC)	
Oral Testimony	10
Prepared Statement	12
Ms. Lori Fena, Chairman of the Board, TRUSTe	
Oral Testimony	19
Prepared Statement	20
Dr. Jason Catlett, President and Chief Executive Officer, Junkbusters Corporation	
Oral Testimony	21
Prepared Statement	23

APPENDIX

STATEMENTS SUBMITTED FOR THE RECORD

The Honorable Howard Colbe, a Representative in Congress From the State of North Carolina	37
The Honorable Howard Berman, a Representative in Congress From the State of California	37
The Honorable John Conyers, Jr., a Representative in Congress From the State of Michigan	38

MATERIALS SUBMITTED FOR THE RECORD

Letter from David C. Quam of Powell, Goldstein, Frazer & Murphy LLP, dated July 19, 2001	40
Letters from Marc Rotenberg and Andrew Shen of Epic.Org, dated February 16, 2001 and July 12, 2001	44

WHOIS DATABASE: PRIVACY AND INTELLECTUAL PROPERTY ISSUES

Thursday, July 12, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 11:05 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble [Chairman of the Subcommittee] presiding.

Mr. COBLE. Good morning, ladies and gentlemen. The Subcommittee will come to order.

Now, today is going to be a chaotic day, folks. I am told there's going to be another vote in about 30 or 40 minutes, so we'll try to get moving here.

Today, the Subcommittee will continue its review of the Internet and domain name policies. The "Whois Database" is the popular name for a combination of information directories. The policies controlling the access and use of this information imply many things, including privacy issues, the ability to enforce intellectual property rights, empowering parents and consumers, aiding law enforcement in public safety activities, and important First Amendment rights.

Some observers have declared that the Internet bubble has burst and have administered last rites to the technology. Still, in many ways, the Internet is thriving and soon will expand even further. Every day more people are going on the Internet. New business models are being launched. Later this year, a variety of new generic top level domains will go online which will encourage new and more diverse activities.

Despite the many positive aspects of the Internet, I am disappointed by the fact that there are many continuing reports of consumer fraud, intellectual property violations, such as cybersquatting, and threats to privacy that occur online. There is a temptation to write more laws in response to these threats. However, I am told that our current legal framework may be adequate to protect the public—as long as the public knows who is the true operator or source behind a given website. It is our hope that as the Internet grows and that these policies develop, the public can count on the availability of a robust and dynamic Whois Database.

Today, we are fortunate to hear from a variety of experts across a variety of disciplines that will help us understand the state of the Whois Database and what it means for copyright owners, trademark holders, privacy organizations, and, in turn, what the Inter-

net means for small businesses and families across America, as well as the public.

It is my hope that they will deliver positive news. I want to assure everyone that this is not the final chapter of the Subcommittee's work overseeing Internet and domain issues. Finally, while I am reluctant to consider introducing legislation, that may be necessary should developments concerning the deployment, content, or access to the Whois Database proves unsatisfactory. As I have stated previously, our Subcommittee has a responsibility to the public—including all of the people who care about privacy, consumer protection, and intellectual property—to guarantee that the Internet develops as a legitimate medium for a range of existing purposes and not as a bazaar for pirates and snake-oil salesmen.

I am now pleased to recognize the distinguished gentleman from California, the Ranking Member, Mr. Berman, for his opening statement.

Mr. BERMAN. Thank you, Mr. Chairman.

The main question involved with the Whois Database—the main questions are what information should be available and to whom should it be available. Policy decisions about the accessibility of Whois information must be made in light of the fact that new domains are now being created, and their creation will exponentially increase the number of copyright and trademark infringing, cybersquatting, and defrauding websites. If new problems like these are going to be created, then mechanisms for addressing those problems should also be created. One such mechanism is access to the Whois Database, and accurate information therein, so that intellectual property owners, fraud busters, and the police can track down those that are taking advantage of these newly created opportunities to break the law. Registries cannot create new problems and then not provide the means to address them.

While the Whois Database is a crucial and necessary tool used by law enforcement, owners of intellectual property, and consumers themselves, this tool can be misused by those who wish to send batches of unsolicited commercial e-mails or commit crimes such as stalking. Where to draw the line between what is necessary for a Whois director and what is an invasion of privacy can be a difficult question.

On either side of the spectrum, I believe that this line-drawing is easy. For websites conducting e-commerce, why should they have a privacy right to keep their place of business and controlling owner a secret? A brick-and-mortar business must get a permit—a permit that is public information—to do business in a city. It seems eminently clear to me that websites conducting e-commerce have very little “right to privacy.”

On the other end of the spectrum, however, a person who has a website for purely personal reasons—pictures of his cat, political complaints against a Member of Congress—shouldn't that person be able to do his personal business without everyone knowing who he is and how he can be found? Isn't political speech worth protecting by redacting the personally identifiable contact information for the website owner? Realistically, however, few websites will meet this ideal of a truly personal endeavor. Furthermore, it's virtually impossible for a registrar to pre-determine which sites are

purely personal, and thus impossible to determine which registrants should be allowed to remain anonymous.

The problem comes in the fact that many websites do not fall at one end of the spectrum. Many businesses are run out of people's homes, for example, and personal websites could have a page on which the owner has illegal digital copies of movies for sale. This latter instance is one that very much concerns me. We are going to hear today about the various ways in which owners of trademarks, patents, and copyrights police their intellectual property over the Internet. Intellectual property owners are concerned about combatting both copyright and trademark infringements on the Internet, and cybersquatting is common enough that being able to find the person behind the site is clearly of extreme importance.

For many IP owners, the Whois Database represents their only line of defense against infringement of their property, and for that reason it is critically important that the information that is in the Whois Database be accurate and verifiable. When I ran my own Whois search earlier this year, I found fraudulent Whois information—a Mr. Angel listed at 1234 Evil Avenue in a city where there is no Evil Avenue, let alone a 1234 Evil Avenue. We may find disagreement about what information should be publicly available, but I strongly believe that what information is there should be accurate.

Thank you again, Mr. Chairman, for calling this hearing.

Mr. COBLE. Thank you, Mr. Berman. I appreciate your statement.

You know, folks, some people in the Congress prefer hearings where you have panelists who are rubber stamps and who agree unanimously upon all issues on the table. It is our belief that we have a better situation when you have a balanced panel, when you have both sides, and that will be the case today. Hopefully, a slugfest will not break out, but we're going to hear from both sides of this issue. It's real good to have all of you with us.

Our first witness today is Mr. Stevan D. Mitchell, who is the vice president of intellectual property policy for the Interactive Digital Software Association. The IDSA is the United States association dedicated to representing the companies that publish video and computer game software which today is a \$6 billion entertainment industry.

Prior to joining IDSA, Mr. Mitchell served as senior counsel to the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. He is a former trial attorney with the section, where he litigated cases under the Computer Fraud and Abuse Act and investigated and prosecuted cases involving illegal uses of technology. In addition, Mr. Mitchell served as a member of the President's Commission on Critical Infrastructure Protection.

Mr. Mitchell earned his law degree from the Florida State University College of Law, where he served as editor-in-chief of the Law Review. He also served as a law clerk in the U.S. District Court for the Southern District of Florida.

Our second witness is Mr. Timothy P. Trainer, president of the Washington, D.C.-based International AntiCounterfeiting Coalition, known as IACC. The IACC represents intellectual property owners

primarily in the trademark, copyright, and patent areas and focuses on intellectual property enforcement issues.

Prior to becoming the IACC president, Mr. Trainer was a staff attorney in the Office of Legislative and International Affairs at the U.S. Patent and Trademark Office. He has also worked on intellectual property enforcement issues as a staff attorney in the U.S. Customs Service and was previously with the law firm of Arter & Hadden.

Mr. Trainer has a law degree from the Cleveland-Marshall College of Law, Cleveland State University. He has lived and studied in Japan and has a master of arts degree in Asian studies from the University of Pittsburgh. In addition, he has written articles and authored a book on intellectual property enforcement issues.

Our third witness is Ms. Lori Fena, who serves as chairman and is co-founder of TRUSTe. TRUSTe is best known for the privacy seal program and has become the most recognized trust brand on the Web. It is credited with innovation in several areas, including private notice, certification, and current systems.

While co-founding TRUSTe, Ms. Fena was the executive director and then chairman of the Electronic Frontier Foundation. Ms. Fena also serves on the policy advisory boards of RealNames and Doubleclick. She has a bachelor of science degree in business information systems from the California State University in Los Angeles.

The Subcommittee is also fortunate to have Dr. Jason Catlett with us today. He is currently president and founder of Junkbusters Corp. He is a nationally known privacy advocate and an expert on technology, marketing, and privacy issues. For those who are not familiar with Junkbusters, it is a private company that assists consumers in identifying and managing information, for example, when e-mail may be "junk" and keep it out of our lives.

Dr. Catlett holds a Ph.D. in computer science, which he taught for several years at the University of Sydney, including courses on technology and privacy. In 1992, he moved to AT&T Bell Laboratories in Murray Hill, New Jersey, where he continued work on "data mining" of large databases. Currently he is a visiting fellow with the Kennedy School of Government at Harvard University. He is a prolific writer and speaker on these issues, including having appeared on the television program "60 Minutes" to comment on privacy and technology.

We are pleased, indeed, to have this outstanding panel with us. Folks, if you will, as you were previously asked to do, if you could confine your remarks, your oral testimony to the 5-minute time frame, we will be appreciative, particularly since there is a vote that will be imminent, I fear. When you see the red light appear in front of you, that is your warning that the guillotine is about to drop, 5 minutes.

Good to have all of you with us. Mr. Mitchell, why don't you kick it off.

STATEMENT OF STEVAN D. MITCHELL, VICE PRESIDENT, INTELLECTUAL PROPERTY POLICY, INTERACTIVE DIGITAL SOFTWARE ASSOCIATION (IDSA)

Mr. MITCHELL. I am Stevan Mitchell, vice president of intellectual property policy with the Interactive Digital Software Association, the IDSA. The IDSA is dedicated to serving the business and public affairs needs of leading publishers of interactive games for video game consoles, personal computers, handheld devices, and the Internet. In 2000, our industry provided jobs for 220,000 Americans and generated nearly \$9 billion in take-home wages and Federal and State personal income tax revenues.

This is a particularly exciting time for our industry. New console formats are expected to propel entertainment software sales from \$6 billion in 2000 to as high as \$16 billion in 2003. At the same time, our members are only beginning to explore new e-commerce markets by creating entirely new online worlds that facilitate multiplayer game play.

This is an industry full of e-commerce pioneers. A serious obstacle to fully achieving the promise of the future, however, is the scourge of online copyright piracy. Every day, thousands of Internet sites pump out pirated copies of video and computer games, undermining legitimate sales and poisoning markets around the world. Copies made available in this way do not just end up in the hands of kids with enough time and inclination to download them. Increasingly, these copies serve as the masters from which thousands more infringing copies are burned to satisfy local market demand throughout the world, all of it illegal and much of it involving establish criminal enterprises.

The industry was most appreciative when, in late 1998, Congress afforded copyright holders a practical, a sensible way to stop some of this bleeding through the notice and takedown provisions of the Digital Millennium Copyright Act. I'm here to tell you that the service that allows notice and takedown to work as Congress intended, is Whois. Restricting access to Whois would not only undermine Congress' goals in enacting the DMCA, it would cripple efforts by content owners to stop illegal theft of their protected works.

In 2000, IDSA investigators used authority provided in the DMCA to achieve approximately 3,000 takedowns of infringing material on the Internet, this in addition to thousands more takedowns initiated individually by our member companies. We estimate that in approximately 90 to 95 percent of these instances IDSA depended on free, unrestricted, real-time access to Whois to further our own investigations. Although essential to notice and takedown Whois is of even greater value where prior notices have failed to put an end to unlawful, often criminal behavior. Whois remains unquestionably the most powerful tool available to help us and our members identify and further investigate recidivist infringers. They're the ones who operate simultaneously using dozens of different domain names and often under different identities. Not coincidentally, they are also the infringers we are most likely to refer to law enforcement for further investigation and criminal prosecution.

If deprived of the ability to use Whois, we would be faced with a difficult choice between two unpalatable alternatives. Do we commence a costly investigation in the absence of Whois data? Or do we instead allow illegal behavior and resulting losses to continue unabated?

We find ourselves facing this uncomfortable and costly choice when we perform Whois queries, only to encounter patently false data. False data persists despite the availability of inexpensive, automated tools to detect it, tools, for example, that would flag when a submitted zip code or area code fails to match up with other information, such as the city name provided at registration.

There is currently no requirement for registrars to assure the quality of data in Whois, although ICANN has the authority to impose such obligations. So as valuable as Whois can be, it can still be improved. We would like to see ICANN work toward making data quality better than it is today.

The other focus of today's hearing is privacy. As I describe more completely in my prepared statement, the IDSA is dedicated to strong private protection online. Nonetheless, we recognize that privacy values must be balanced between other societal values and concerns. In reflecting on this balance, this Subcommittee should consider how many other socially beneficial purposes, apart from intellectual property protection, are served by keeping Whois data publicly accessible.

My written statement describes the myriad benefits inuring to companies and consumers and families through free, unrestricted, real-time access to Whois data.

With respect to e-commerce, publicly available Whois data instills accountability and bolsters confidence among participants to commercial transactions. Even so, it remains the case that much less personally identifiable information is required to engage in commerce on the Internet than must be surrendered in order to open a business on Main Street.

Considering these benefits, it would be inappropriate to wall off or restrict access to Whois to protect privacy on the Internet. Currently and developing privacy laws, policies, and practices are entirely compatible with maintaining the status quo of publicly accessible Whois. There is a legitimate role for anonymity online, but that role can be fully realized without undermining the fundamental precept of public accountability to Whois data.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF STEVAN D. MITCHELL

Mr. Chairman, and Members of the Subcommittee:

Thank you for this opportunity to testify on behalf of the Interactive Digital Software Association (the IDSA).

The IDSA is exclusively dedicated to serving the business and public affairs needs of companies that publish video and computer games for video game consoles, personal computers, handheld devices and the Internet. IDSA members collectively account for more than 90 percent of the \$6.0 billion in entertainment software sold in the U.S. in 2000, and billions more in export sales of entertainment software. In 2000, our industry provided jobs for 220,000 Americans and generated nearly \$9 billion in take-home wages and federal and state personal income tax revenues. The entertainment software sector is one of the fastest-growing and most dynamic parts of the U.S. economy.

This is a particularly exciting time for our industry. New entries in the console market are expected to propel entertainment software sales to as high as \$16 billion

a year by 2003. At the same time, our members are only beginning to explore new e-commerce prospects by creating entirely new online worlds that facilitate multi-player game play.

Of course, as this Subcommittee well knows, one of the biggest threats to the continuation and growth of this American success story is piracy, which robs our companies of billions of dollars of revenue annually worldwide. Online piracy is one of the most disturbing and damaging aspects of this scourge. Every day, thousands of Internet sites are pumping out pirated copies of our copyrighted video and computer games, undermining legitimate markets around the world. Enforcement against this rampant online piracy of our products is one of the greatest challenges facing our industry today.

The IDSA and its members companies are meeting that challenge through an aggressive self-help effort and a growing Internet enforcement capability. Today's hearing focuses in large part on an essential tool for our efforts to enforce copyright protection online: WHOIS.

In 2000, the IDSA used authority provided in the Digital Millennium Copyright Act (DMCA) to achieve approximately 3000 "takedowns" of infringing material on the Internet. Over the last year we also filed 10 civil lawsuits against Internet pirates as enforcement actions on behalf of our members, assisted in additional actions brought by member companies, and made a number of criminal referrals to law enforcement. This is in addition to thousands more takedowns and numerous lawsuits initiated individually by our member companies. These accomplishments are reflective of similar successes reported by the other copyright-based industries. DMCA self-help allows us to reduce to a fraction the losses we would suffer if limited only to court-imposed process and remedies.

These efforts are made much less effective without the unrestricted access we currently have to WHOIS data, including contact information regarding domain name registrants. In past hearings, this Subcommittee has already heard a lot of testimony (including from the IDSA in 1999) about how copyright owners use WHOIS data to identify and locate the parties responsible for operating pirate Internet sites. I would like to emphasize today that we chiefly use WHOIS data to help identify the Internet Service Provider (ISP) responsible for hosting a pirate site. Armed with this information, we can then invoke the "notice and takedown" procedures of the DMCA to ensure that the online pirate is taken offline quickly and efficiently. Congress, led by this Subcommittee, have given us an invaluable anti-piracy tool in the DMCA; but that tool would not be as reliable, efficient and effective without continued free, unrestricted, real-time public access to WHOIS data.

What I have said about the importance of WHOIS access to the IDSA's online enforcement efforts also applies to the other trade associations representing copyright owners, as well as to individual copyright holders who undertake efforts to combat Internet piracy. We work with nine other organizations in the Copyright Coalition on Domain Names (CCDN), for the primary purpose of maintaining and strengthening public access to WHOIS. Each of us share an abiding appreciation for the importance of WHOIS for reasons outlined by the IDSA back in 1999, in the March testimony of Steve Metalitz, Counsel to the CCDN, and here again today.

WHOIS serves a valuable function with respect to notice and takedown. But it also helps us take those next few steps in instances where prior notices have not put an end to the unlawful, often criminal behavior. WHOIS is unquestionably the most powerful tool available to help us identify and investigate recidivist infringers. These are the ones who operate simultaneously using dozens of different domain names, and often under different identities. (Not coincidentally, these are also the infringers we are most likely to refer to law enforcement for criminal prosecution.)

One of our member companies described to us an unfortunately all-too-common scenario where piratical activity occurring on multiple sites appeared to be unrelated, until they were able to query WHOIS and analyze the data for common denominators (such as different names but same addresses for registrants, identical administrative or technical contacts, common servers, etc.).

Here WHOIS empowers intellectual property owners to do more to further an investigation and isolate the most recalcitrant offenders for follow up by law enforcement. A more robustly searchable WHOIS database would be even more valuable in this regard.

WHOIS is also extremely valuable to our members in monitoring use (and abuse) of their registered trademarks. After locating online questionable use of their marks, WHOIS provides a way to facilitate initial contact with the parties in question, individual-to-individual and company-to-company, helping in many instances to achieve amicable resolution and avoid expensive investigative and litigation costs.

It follows that we are not only concerned about public accessibility of these databases, but with the breadth and quality of the information they contain. Some Top

Level Domains (TLDs) outside the .com/.net/.org arena provide only a limited subset of WHOIS data, or none at all. For instance, the British country code TLD, .uk, provides virtually no registrant contact data beyond the name of the registrant. When we seek to protect the intellectual property rights of our member companies against piracy emanating from the .uk domain, we are faced with a difficult choice between two unpalatable alternatives: Do we commence a costly investigation in the absence of WHOIS data, or do we instead allow patently illegal behavior and resulting losses to continue unabated? Of course, we sometimes face a similar Hobson's choice in the .com environment, whenever the WHOIS data which we are able to access is obviously false.

The other focus of today's hearing, of course, is privacy. Privacy is not just a buzzword for the IDSA. It is part of the tool kit we provide to our members and the public to make privacy work on the net.

Through the Entertainment Software Rating Board (ESRB), an independent, self-regulatory body created by the IDSA in 1994, we make available to companies the ESRB Privacy Online Program. The program assists companies that transact business online to protect consumer information exchanged via the Internet. This voluntary program includes privacy principles and guidelines, an oversight and enforcement regime, a consumer grievance procedure, and a consumer-oriented alternative dispute resolution mechanism.

The program has proven successful despite its rigor, as demonstrated by the Federal Trade Commission's recent approval of ESRB Privacy Online as a "safe harbor" under the Children's Online Privacy Protection Act. ESRB Privacy Online was the first privacy seal provider to receive such approval from the FTC under the law.

Thus, the IDSA is both an organization dedicated to strong privacy protection online, and an organization that relies upon continued unrestricted public access to WHOIS data to protect the intellectual property rights of its members and their continued contribution to U.S. jobs and the economy. As such, I believe we are well positioned to comment on the subject matter of this hearing, which is the intersection of WHOIS and privacy.

With respect to privacy concerns, we believe strongly that publicly accessible WHOIS is fully compatible with generally accepted principles of privacy protection. That's because privacy is never an absolute, but is a value that must be balanced with other important social objectives. When we carry out that balancing process, it's not hard to see why publicly accessible WHOIS has coexisted peacefully with privacy laws and policies for many years—in fact—since the inception of the domain name system more than a decade ago. We believe that this successful balance and coexistence must be maintained.

In striking the balance, it's important to recall how many other socially beneficial purposes—apart from intellectual property protection—are served by keeping this data accessible to the public. Those purposes can be summed up in two words: accountability and transparency. WHOIS enables consumers, parents, and all Internet users to know with whom they are dealing when they venture online. And that transparency provides a measure of accountability that helps to ensure that the Internet can be a safe, enjoyable, and worthwhile place to visit and live.

Let me give a few examples of some of the other beneficial functions that depend on continued public access to WHOIS.

WHOIS provides an essential capability to network operators and security personnel to identify system problems and track down those seeking to propagate computer viruses or otherwise cause harm. Network security is a paramount concern to our member companies, whose online gaming worlds are built to utilize and protect the confidentiality, availability and integrity of host systems and user data. In a broader context, to the extent that WHOIS is used to identify and pursue those who would seek to compromise sensitive company data, or an individual's data or communications, then public access to WHOIS is a tool that promotes privacy protections.

WHOIS' value as a consumer protection cannot be overstated. It empowers consumers to discover who they are dealing with and to pursue redress for grievances. The fact that WHOIS data is publicly available by itself serves the important function of instilling accountability and bolstering confidence among participants to commercial transactions. This is particularly important in the online world, where consumers lack other indicia of reliability, such as storefront appearance and on-hand inventory, and where an Internet "storefront's" net address can be far more transitory than a brick-and-mortar Main Street address. This function underscores the need to keep WHOIS data accessible to every consumer, as well as to the myriad government and non-profit agencies that help to promote better business practices and to enforce the consumer protection laws online.

Users of WHOIS are not confined to the commercial world. Many concerned parents regularly make use of WHOIS capabilities to learn more about websites and other Internet resources used by their families. The sources of inappropriate online content can be much more easily identified so long as WHOIS remains generally available to the public.

One argument you may hear is that the same WHOIS database that so effectively serves rightsholders, consumers and the public can be misused as a source from which to harvest email addresses for spamming purposes. The IDSA has no interest in promoting this use—or should I say abuse—of publicly accessible WHOIS data. We need to be able to make specific queries of the WHOIS database and to get a limited number of responses in real time. Spammers, by contrast, need bulk access to the entirety of the WHOIS database—or at least to a huge chunk of it—in order to fulfill their objectives. The current ICANN rules on WHOIS access recognize this distinction.

Because of the extensive public benefits that flow from unrestricted public access to WHOIS data, we do not believe it is necessary to wall off or restrict access to WHOIS to protect privacy on the Internet. Current and developing privacy laws, policies and practices are entirely compatible with maintaining the status quo of publicly accessible WHOIS. There is a legitimate role for anonymity online, but that role can be fully realized without undermining the fundamental precept of public accessibility to WHOIS data.

We should keep in mind that WHOIS is simply the contact data for registrants of “second level domains”—those who are responsible for what appears immediately to the left of the “dot” in an Internet address. For example, in the address “idsa.com,” the second level domain registration involves the characters “idsa.” WHOIS data does not reveal the party responsible for any other aspect of an Internet address, whether it involves further subdomains to the left of the second level domain name, or specific locator information for an Internet site that may appear to the right of “.com” following backslashes or other punctuation marks. Nor does WHOIS data tell the public anything directly about the person behind a specific e-mail address: in other words, WHOIS does not venture to the left of the @ sign.

I take this excursion into technicalities simply to suggest that there are many opportunities for individuals to establish and maintain an anonymous online presence without any need to cut off or restrict public access to WHOIS data. Beyond a certain level of online activity, however, we reach a point at which an insistence on a right to anonymity is no longer appropriate.

Certainly once one decides to exploit the Internet as a medium for commercial transactions or other business opportunities, the need for accountability and consumer protection demands that basic contact information should be available and accessible. Requiring a party who wants to use his or her Internet presence for such transactions to provide the most basic of reliable contact information is a perfectly reasonable condition of entry to the online marketplace. Making that basic contact information available to the public is a basic protection for consumer online, whether the parties they are dealing with are individuals or companies, and regardless of whether money changes hands in a particular transaction. Even so, it is still the case that much less personally identifiable information is required to engage in commerce on the Internet than must be surrendered in order to open a business on Main Street.

We are also confident that a similar balance between anonymity and accountability to support e-commerce can be found in the international and national legal standards for privacy or “data protection.” Those standards are evolving, but privacy laws are not brand new, and we have enough experience to be able to say that publicly accessible WHOIS can peacefully coexist with even the most aggressive privacy laws now on the books.

To our knowledge, no governmental privacy authority has ever officially objected to the real-time, unrestricted public accessibility of WHOIS data in the .com/.net/.org environment, even though the registrars who maintain these databases are located in more than a dozen different countries, each with its own privacy laws and policies. There have been comments, there have been concerns, but there have never to date been any collisions between data protection or privacy laws and publicly accessible WHOIS policies.

This is true even in the case of the European Union’s Data Protection Directive, which, as the Subcommittee knows, is much more restrictive of the free flow of information than anything comparable in the U.S. The EU Data Protection Directive does embrace the general rule that individuals can prevent access to information about themselves, such as name, address, and the like, which is contained in the WHOIS database. But Article 7 of the Directive makes this rule subject to a number of exceptions, several of which are highly relevant here. These exceptions range

from consent to several other provisions under which privacy must be balanced against a number of other critical factors, including the legal obligations of the data controller (in this case, the domain name registrar or registry); performance of tasks carried out in the public interest; and the legitimate interests of parties to whom the data may be disclosed. In other words, in Europe as in other jurisdictions, striking the right balance allows the long-standing public accessibility of WHOIS to remain in force.

The most recent developments in the ICANN roll-out of new Top Level Domains underscore this conclusion. Both of the new TLDs which have started up operations so far—.biz and .info—have pledged to make their WHOIS data available to the public, without charge, in real time, and have not encountered any difficulties either with ICANN-accredited registrars in the various countries nor with data protection authorities.

A third new TLD—.name—is based in the United Kingdom and has consistently sought, in its proposed policies, to comply fully with the U.K. privacy laws. After extensive discussions with intellectual property interests and others, .name has arrived at a proposal that it believes to be fully compatible with those laws. This proposal is acceptable to the intellectual property community because it does not substantively diminish the breadth of contact data about domain name registrants to which copyright owners, consumers, parents, and other members of the public will have free, real-time, unfettered access in the .name environment. If the .name WHOIS policy is finalized on this basis, it will powerfully demonstrate the compatibility of the European approach to data protection with the public's need for unrestricted access to WHOIS.

This brings us to three “takeaway” points we would like the Subcommittee to keep in mind in discharging its oversight responsibilities.

First, this Subcommittee should maintain close oversight of public accessibility to WHOIS data. This issue will have to be addressed each time ICANN adds another new Top Level Domain (TLD). We believe that the new TLDs added so far have adopted policies on WHOIS that are at least adequate. But neither of these new TLDs (.biz and .info) has yet “gone live,” and agreements have not yet been concluded between ICANN and the other new registries. The message that Congress expects every new TLD to assure at least a minimum level of accountability and transparency through publicly accessible WHOIS must be reiterated each time: to the Commerce Department (which is the lead Executive Branch agency), to ICANN, and to the new registries themselves.

Second, I urge the Subcommittee to be vigilant about the impact of any U.S. privacy legislation on robust WHOIS functionality. We need to make sure that any statutory standards adopted here do not inadvertently impede the healthy development of electronic commerce. Free, real-time public access to WHOIS data must be preserved and strengthened, not undermined.

Finally, I must mention the situation in the country code Top Level Domains (ccTLDs). This is the fastest-growing part of the domain name system; yet the level of public access to registrant contact data in many of these domains is woefully inadequate. As the ccTLDs are brought under the ICANN umbrella, we must ensure that they accept fair ground rules for their operation, including public accessibility of registrant contact data. The U.S. Government will have a critical role to play in establishing this core concept, and active oversight by this Subcommittee will be essential.

I thank the Subcommittee for the invitation to appear here today and for this Subcommittee's unwavering commitment to the protection of intellectual property rights.

Mr. COBLE. Thank you, Mr. Mitchell. Mr. Mitchell, I gave you an extra 45 seconds, so in the sense of fairness, I will be equally liberal with the rest of you.

Mr. Trainer, you are recognized for 5 minutes and 45 seconds.

**STATEMENT OF TIMOTHY TRAINER, PRESIDENT,
INTERNATIONAL ANTICOUNTERFEITING COALITION (IACC)**

Mr. TRAINER. Thank you, Mr. Chairman.

Mr. Chairman, Congressman Berman, good morning. On behalf of IACC members, I thank the Committee for the opportunity to testify on an important issue affecting intellectual property owners, Internet users, and the public at large—the availability and use of

identification information that registrars collect from domain name registrants.

The IACC is the largest organization dealing exclusively with IP piracy and counterfeiting issues. Total annual revenues of IACC members exceed \$650 billion and represent a cross-section of industries, including the automotive, entertainment, apparel, and pharmaceutical sectors, and many others. These diverse industries have a common objective: protecting intellectual property rights and customers from counterfeiters and pirates.

Mr. COBLE. Mr. Trainer, if you'd pull that mike a little closer so that the folks in the back of the room can hear you. Thank you.

Mr. TRAINER. Given the limited time we have today, I begin with our recommendations for improving Whois and increasing protections for consumers and IP owners.

First, Whois Database operations must continue to be mandatory for all ICANN-accredited registrars, regardless of the gTLD the registrar is managing; and, second, registrars must obtain and maintain basic contact information which must be publicly accessible, verifiable, and kept up to date. And we elaborate more on these in our written testimony.

Supporting my first point, our position is that the availability of registrant information is critical to IP owners for enforcement of their rights over the Internet and to providing consumers with some recourse against counterfeiters and pirates. This Committee understands the importance of intellectual property in today's global economy. Although the IACC and others have advocated increased law enforcement efforts to protect IP rights, nearly 99 percent of all enforcement is done civilly by owners.

Unfortunately, the Internet has complicated efforts to protect intellectual property rights. Just as the Internet opened new markets for legitimate companies, it also opened new markets for counterfeiters and pirates. IACC member companies, who once considered mega-flea markets as their biggest problem, now point to the Internet as the greatest threat to their brands. Why? Because the Internet eliminates key indicators like location, quality, and personal interaction with a vendor that consumers and investigators use to identify fakes in the physical world. In cyberspace, the virtual store, digital imaging, and point-click purchasing often leave investigators and consumers blind and uninformed.

Until another method of identifying those behind certain websites is created, Whois remains the only tool for companies looking to protect their intellectual property rights on the Internet. Thus, for our members, the importance of an open, accurate, and accessible Whois Database cannot be overstated.

Regarding the interaction of IP rights and privacy rights, the IACC believes that the current system is fairly balanced between IP owners and consumers and the privacy interests of domain name registrants. When you conduct a Whois search for a domain name owner, the information you see is the name and address of the owner of that domain name. This is the information we found when we conducted some random Whois searches: You see no telephone or facsimile numbers of the domain name owner, no e-mail addresses, certainly no tax identification number, no Social Security number, no other personal information. In effect, a filtering

mechanism is in place. The information that is accessible is not sufficient in and of itself to result in the types of Internet privacy crimes one reads about, such as identity theft. In essence, the Whois Databases provide only the most basic information about the domain name owner.

The current balance between privacy and access is a fair one for several reasons. First, domain name ownership is not a right. Second, a person making a decision to have a presence on the Internet, perhaps the most public forum in existence, should have a lowered expectation of privacy. Third, with all ICANN-accredited registrars, a domain name registrant gives consent to providing public access to some information. And, fourth, although privacy is important, it is not an absolute right that should trump all other social values.

If the current balance between publicly available Whois information and privacy were tipped toward greater privacy protections, how would intellectual property owners protect their rights? If information about domain name owners were not available because of a strict privacy policy, how would trademark owners have gathered information they needed to bring the nearly 4,000 domain name dispute cases handled under the existing uniform dispute resolution policy last year?

Congress cannot require IP owners to enforce their rights, then take away the tools needed to do the job. An open, accurate, and accessible Whois Database, with the limited information it requires, strikes the proper balance between privacy interests and the need for IP owners to police their intellectual property.

Finally, it is the IACC's position that registrars should be responsible for keeping the database accurate. ICANN-accredited registrars are obligated by an agreement to collect, maintain, and furnish to the public the domain name owner contact information. It is time to enforce those obligations by considering a failure by a registrar to take steps to verify and reverify contact information as a breach of the accreditation agreement. We also strongly suggest that the U.S. Government urge ICANN to pay more attention to the implementation and enforcement of the registrar's agreement obligations and increase its efforts to restore Whois, at least to the level of usability that the public enjoyed up until the advent of registrar competition in 1999.

As critical as the Whois Database is to IP owners and consumers, the database is only as useful as the information it contains. We urge this Committee to closely monitor the ICANN process and make accuracy a key component of Whois discussions.

Thank you again for this opportunity to provide these comments on behalf of the IACC. I'd be happy to answer any questions you may have.

[The prepared statement of Mr. Trainer follows:]

PREPARED STATEMENT OF TIMOTHY P. TRAINER

Mr. Chairman and Members of the Subcommittee, Good morning. I am Timothy Trainer, President of the International AntiCounterfeiting Coalition (IACC). On behalf of the IACC, I would like to thank the Committee for the privilege and opportunity to testify on an issue of great importance to intellectual property owners, Internet users, and the public at large—the collection, availability, and use of identification information collected from domain name registrants by domain name registrars.

The IACC is the largest organization dealing exclusively with issues involving intellectual property piracy and counterfeiting. The IACC has approximately 160 members who represent a cross-section of industries, including the automotive, electrical, motion picture, software, sound recording, apparel, luxury goods, personal care and pharmaceutical sectors. The total annual revenues of IACC members exceed US\$650 Billion. The objective that brings such diverse industries together is their need to protect their intellectual property and their customers from those who would steal such property.

I am also personally thankful for the opportunity to testify because I was involved in the discussions that led to the issuance of the Department of Commerce's Green and White Papers on changes to Domain Name System (DNS) management during my service in the U.S. Patent and Trademark Office's Office of Legislative and International Affairs. Now as a member of the private sector, my opinion has not changed: WHOIS must remain open, accessible and accurate. Consequently, my testimony will address the following topics:

What is commonly referred to as the WHOIS database is the collection of information gathered by a domain name registrar from domain name registrants. Currently, there are approximately 150 domain name registrars that are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN). Accredited registrars are "bound" by the terms of the ICANN Registrar Accreditation Agreement (RAA). Sections II.E and II.F of the RAA require registrars to collect, maintain, and make available to the public information regarding each second level domain (SLD)¹ they register.²

To companies and consumers, WHOIS is an identifier. It is the address on the front door or the license plate on the car. If a businessman wants to acquire a domain name, if a parent wants to know who owns the website that is distributing harmful toys, if a consumer wants to know who owns the website that is offering discounted pharmaceuticals, or if a trademark or copyright owner wants to know who owns the domain name from which a counterfeit version of its products are being sold, they have one place to turn—the WHOIS databases.³ Consequently, the

¹A generic top-level domain or gTLD is commonly understood as the .com, .org, .net, etc. ending, which an accredited registrar manages, in cooperation with ICANN. The SLD is the domain name a third party registers with the accredited registrar, i.e., iacc.org.

²II.F. *Public Access to Data on SLD Registrations*. "During the term of this Agreement:

1. At its expense, Registrar shall provide an interactive web page and a port 43 WHOIS service providing free public query-based access to up-to-date (i.e. updated at least daily) data concerning all active SLD registrations sponsored by Registrar in the registry for the .com, .net, and .org TLDs. The data accessible shall consist of elements that are designated from time to time according to an ICANN-adopted policy. Until ICANN otherwise specifies by means of an ICANN-adopted policy, this data shall consist of the following elements as contained in Registrar's database: The name of the SLD being registered and the TLD for which registration is being requested;
 - a. The IP addresses of the primary nameserver and secondary nameserver(s) for the SLD;
 - b. The corresponding names of those nameservers;
 - c. The identity of Registrar (which may be provided through Registrar's website);
 - d. The original creation date of the registration;
 - e. The expiration date of the registration;
 - f. The name and postal address of the SLD holder;
 - g. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the SLD;
 - h. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the SLD."
2. Upon receiving any updates to the data elements listed in Sections II.F.1.b through d and f through i from the SLD holder, Registrar shall promptly update its database used to provide the public access described in Section II.F.1.

³Prior to 1999, Network Solutions, Inc., both managed the Domain Name System (DNS) and registered SLDs under contracts with the U.S. Government. Once the monopoly was broken, ICANN accredited dozens of registrars (currently, there are approximately 160), and each of them began building their own, separate WHOIS database. Although services such as *www.better-WHOIS.com* and *www.allWHOIS.com* allow an inquirer to search multiple registrars online and free-of-charge, the data is still flawed and no single system exists to allow the search of all accredited registrars, let alone the registrant databases maintained by unaccredited registrars and those who manage the country code TLDs (ccTLDs—which currently number approximately 240). In negotiations to revise its contract to run the .com/net/org registry, Verisign agreed to devote part of a \$200 million research and development fund to work on a "universal WHOIS" to allow access to WHOIS data from as many registries as possible (.com/net/org, new TLDs, ccTLDs) via a single portal. Work is to begin this year with the goal of making substantial progress by the end of 2002. Whether this system is a valuable tool or

IACC believes that Congress and the Administration should continue to advocate for an open and accessible WHOIS database for all Internet users and strive to improve the accuracy of the information contained therein.

In support of this position, my testimony will focus on the following topics:

1. The compatibility of reasonable privacy interests with the maintenance and accessibility of “WHOIS” databases;
2. The importance of publicly accessible “WHOIS” information; and
3. The need to ensure that “WHOIS” information is current and correct by either enforcing existing obligations or imposing new ones.

I. Whois vs. Privacy

The IACC endorses a policy that enables intellectual property owners, consumers, parents and other interested persons to obtain, at the very least, the type of information currently available in the WHOIS databases. It is our position that the current system is fairly balanced between consumers right to know and a domain name registrant’s expectation of privacy. In fact, if anything, the IACC believes that registrants should be required to improve their performance in insuring that domain name registrants provide correct and updated information. Because a person (legal or individual) voluntarily chooses to be present on the Internet, the identity and contact information of domain name registrants are entitled to no more privacy protection than are business or home addresses in the physical world.

Privacy advocates concede that accurate domain name lookups are essential. In a February 16, 2001 letter to Congress, Mr. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC) stated, “For good reasons related to the technical and security considerations of maintaining websites and domains, it is necessary to make such information publicly available. Making such contact information available has been the practice of the domain name process for many years and is well-accepted by the many in the Internet community.”⁴ Mr. Lauren Weinstein, Moderator of the Privacy Forum and Co-Founder of the People for Internet Responsibility, has expressed the opinion that he opposes limiting access to WHOIS information or allowing registrants to withhold phone numbers. He was quoted as saying, “In tracking down privacy, spam, or network problems, when things go wrong, you’ve got to be able to call someone. You can’t always rely on email. So, what are you going to do, send them a letter?”⁵

The IACC agrees, however, that certain practices permitted under the ICANN Registrar Accreditation Agreement (RAA) contribute to abuses and inappropriate use of personal information.⁶ The RAA, however, already has mechanisms that registrars can enforce in order to reduce these abuses.⁷

A close examination of the information that is currently available about the domain name registrants leads us to no more than the name and address of the domain name owner. It is important to understand what one gains access to when a WHOIS search is conducted. Specifically as it relates to the domain name owner, the only information that one sees is the owner name and an address. As an example, if one looks up the IACC’s domain name registration, the only information a person will see is our name and address. There is no telephone number, facsimile number or email addresses for staff members. In effect, there is a filtering mechanism in place from the outset.

It is also important to understand what is not available. For example, one cannot find a business’s tax identification number or an individual’s social security number or other personal information. Therefore, the information that is accessible is not sufficient in and of itself to result in the types of Internet crimes that make up identity theft. In essence, the WHOIS databases provide very little information about the domain name owner.

is redundant of the existing “WHOIS portals,” remains to be seen. (See footnote below on privacy complaints regarding Verisign’s marketing of WHOIS data).

⁴EPIC letter to Senators Conrad Burns and Fritz Hollings and Representatives Fred Upton and Edward J. Markey, criticizing VeriSign’s (formerly Network Solutions, Inc.) aggressive marketing of WHOIS registrant information. www.epic.org/privacy/internet/ICANN-privacy.html. ICANN is currently considering proposals to limit the RAA’s existing rules governing mandatory bulk access of registrant data.

⁵Reported April 5, 2001 in InternetNews at www.internetnews.com/bus-news/article/0,,3-734951,00.html.

⁶Registrar Accreditation Agreement (RAA), II.F.6.a “Registrar shall make a complete electronic copy of the data available at least one time per week for download by third parties who have entered into a bulk access agreement with Registrar.”

⁷RAA, II.F.6.d and e.

In the balancing of interests between privacy and access to information, a person's decision to be present on the internet should lower the expectation of privacy because the Internet is the most public place in existence. A single person can be present simultaneously in each country that has a computer online. Moreover, domain name registrants obtaining domain names with accredited registrars consent to providing a certain amount of information with the knowledge that some information will be available to the public.⁸

Without the proper balance between publicly available information and privacy, what could intellectual property owners do to protect themselves? If information about domain name owners were not available because of a strict privacy policy, what alternative would trademark owners have had in the nearly 4,000 domain name dispute cases that have been handled under the current Uniform Dispute Resolution Policy?⁹ If trademark owners had been denied access to information identifying domain name registrants because of privacy, the only recourse would be to place their hopes on law enforcement. Thus, it is both wise policy and a necessary requirement to have information available to the public, including intellectual property owners, so that both private citizens and businesses can protect themselves and not be wholly reliant on government resources. Governments have neither the resources nor the desire to be dragged into thousands of legal controversies that could be otherwise resolved by providing basic identification information about those on the World Wide Web.

There are many ways for individuals to establish a robust presence on the Internet without even registering a domain name themselves. Those individuals who choose to register a domain name should not be exempt from the mechanisms (like WHOIS) that serve to bring a minimum level of accountability and transparency to online activities that may impinge on the rights of others. Few people, and virtually no laws, treat privacy as an absolute right that trumps every other social value. Unrestricted public access to WHOIS data—the long-established status quo in the generic TLDs—is fully consistent with a balanced approach to privacy.

The IACC is not aware of any privacy or data protection law in the world that guarantees absolute anonymity for all of a person's activities that bring him or her into contact with others. Existing laws recognize a number of exceptions that justify public access to WHOIS, including registrant consent, legal obligations to disclose, or disclosure for the purpose of carrying out a contract to provide services. Furthermore, there are means by which a domain name registrant may maintain anonymity (such as by use of a third level domain in the existing gTLDs), so long as a registrant whose contact data is available accepts full legal responsibility for the activities of the anonymous registrant.

Ownership of a domain name is not a right. Rather, a domain name is an identifier that an individual or a company, in effect, leases, although that lease is commonly discussed in terms of ownership. In exchange for the ability to use this means of identifying oneself, one's place on the Internet, a registrant is asked to provide certain information. Just like a business owner seeking a storefront, or a citizen seeking a home, certain information about the location of a business or home is available in public records; hence, the same should occur in the case of domain names. As in the physical world, if a person transacts legitimate or illegitimate business, if he or she offers information or services, or if his or her presence at all affects other people's lives, those affected should have the mechanism available to contact a designated person who can respond to inquiries, complaints, or notice of process.

Not long ago, we were calling the Internet the "information superhighway." Websites are like cars on that highway. Sometimes, cars obey the rules, sometimes they don't. Their presence always has consequences—good or bad, intended or unintended. In the physical world, in a hit and run situation, in a case of speeding through a neighborhood, or otherwise driving recklessly, how do victims or those endangered by the driver's conduct know who is responsible? We know by the license plate—the number and State of registration. The domain name is to a website what license plate is to a car. An identifier behind which stands information about the owner of the car and is fully available to anyone who wants or needs it.¹⁰

⁸ RAA, II.J.7.

⁹ A check of the proceedings brought under the ICANN Uniform Dispute Resolution Policy, the data indicated that 3,978 proceedings had been initiated as of July 6, 2001, involving over 7,000 domain names.

¹⁰ The driver's license analogy has been used in the past to justify the collection of information for the WHOIS database. The IACC believes that the license plate analogy more accurately reflects the dimensions of this issue.

Likewise, although there may be First Amendment protections for the contents of a website, the other passengers on the “information superhighway” are entitled to know in whose name the “car” is registered—who is the registrant of the SLD. Just as in the physical world situation, if a civilian or a law enforcement official invades the registrant’s privacy, there is recourse. The default position should be that the information is public and those who commit transgressions with the information will be subject to consequences.

The automobile registration database, like a WHOIS database, is only as good as the information given at the time of registration. It is reasonable to assume that jurisdictions that have rules to ensure that accurate information is given have a better chance when it comes to enforcing the law than do those jurisdictions that do not have or do not enforce requirements.

With regard to the assertion that the WHOIS databases contribute to the proliferation of bulk mail on the Internet, the IACC has two observations. First, this is not clearly the case, as many bulk mailing lists are “harvested via customizable programs that trawl websites and mailing lists,” according to Paul Kane, Chairman of the WHOIS Committee, a committee of ICANN’s Domain Name Supporting Organization. The WHOIS databases are not generally used in cases involving unsolicited, bulk mailings (SPAM).¹¹

Second, as stated above, the RAA includes provisions instructing registrars about third-party bulk access and the limitation on the use of the WHOIS data.¹² Thus, in view of the provisions that already exist, there is no reason to lower thresholds for personal accountability in Internet conduct. We should not sacrifice the ability to see who is behind a domain name just because conduct takes place on the Internet. Even advocates against the proliferation of unsolicited, commercial email concede that the WHOIS database plays a crucial role in helping victims identify the sources of SPAM and other online transgressions.¹³

Certainly, a distinction can be drawn between commercial or public speech transmitted to the public via a website, i.e., an online bookstore or a political action site, and “personal” speech, albeit transmitted in a public way, i.e., a website of family photographs available to family members worldwide. However, the privacy interests inherent in the “luxury” of owning a website must be balanced against the public’s need to know who is on the Internet. Compared to the types and quantity of information requested for other activities in life which are difficult, if not impossible to live without, a drivers license, medical insurance, marriage license(s), each of which is accorded different levels of privacy protection, the WHOIS databases collect a minimal amount of information in connection with an activity that most people could live without—ownership of a domain name.

Given the global reach of the Internet, and the potentially broad intended or unintended effects of a presence on the Internet, WHOIS information should be open, accurate and accessible to intellectual property owners and other interested persons, including consumers and parents. The publicly available information is a minimal amount when compared to all of the personal identification that attaches to individuals in today’s world.

II. The Importance of “Whois”

It is the IACC’s position that the availability of registrant information is critical to allowing IP owners to enforce their rights over the Internet and for providing consumers with some recourse against counterfeiters and pirates.

This Committee knows full well the importance of intellectual property to today’s companies and the fact that the burden for protecting such property rests largely with the IP owner. Although the IACC and other intellectual property groups have advocated for greater enforcement of IP rights by law enforcement, nearly 99 percent of all enforcement is done civilly by the IP owner.¹⁴ Unfortunately, for all its

¹¹The Washington Post, June 11, 2001, www.newsbytes.com. In fact, even the sale of WHOIS information is restricted to certain purposes by the RAA (discussed above). Sections II.F.5 and 6.c prohibit registrars from providing WHOIS contact data to third parties if that information is to be used to “allow, enable, or otherwise support the transmission of mass, unsolicited, commercial advertising or solicitations via email (spam).” Furthermore under RAA Sections II.F.6.e and f, registrars may require third parties not to resell the data unless it has been transformed through incorporation in a value-added product, and may enable SLD holders who are individuals to “opt-out” of the bulk access database. Again, enforcement of the existing provisions seems to be the key to solving many apparent problems with management of the domain name system (DNS).

¹²RAA, II.F.6.c.

¹³The Washington Post, June 11, 2001 The article refers to the comments of Jason Catlett, President of Junkbusters (www.junkbusters.com).

¹⁴According to published reports, in FY2000, DOJ convicted 44 individuals of criminal trademark violations under 18 U.S.C. 2320.

promise, the Internet has made the IP owners' burden to protect their marks more difficult. Just as the Internet opened new markets for legitimate companies, it also opened new markets for counterfeiters and pirates. IACC member companies, who used to consider mega-flea-markets as their biggest problem, now point directly at the Internet as the greatest threat to their brands. One reason for this is that the Internet did away with some of the key indicators that investigators and consumers used to detect counterfeit merchandise. Indicators such as location, quality, and personal interaction with the vendor are key to identifying fakes in the physical world. In Cyberspace, however, the virtual store, digital imaging, and point-click purchasing often leave investigators and consumers blind and uninformed.

The one investigative element that IP owners have in the Internet marketplace is WHOIS—a necessary point of contact in an artificial world. IP owners use the information in the WHOIS database in a number of ways. Sometimes they approach the site operator directly, with a demand that the unlawful activities cease. Sometimes WHOIS data is used to track relationships between websites to “map” IP infringers' activities and “business” associations. This information can be used to establish whether a particular infringer is engaged in a pattern of behavior, such as a cybersquatter's wholesale warehousing of domain names that are confusingly similar to trademarks, or other types of IP crimes. Such information can also be useful in later civil or criminal enforcement proceedings, or as leverage in settlement discussions. WHOIS also allows copyright owners to invoke the Digital Millennium Copyright Act's “notice and takedown” procedure and is used by trademark owners to help demonstrate a cybersquatter's bad faith.

Until another method of identifying those behind certain websites is created, WHOIS remains the only tool for companies looking to protect their intellectual property rights on the Internet. Thus, the importance of an open, accurate and accessible WHOIS database cannot be overstated in view of all the interested persons relying on these databases.

III. Making WHOIS Current and Correct

It is the IACC's position that registrars, as the sole entities that can collect, verify, and maintain the information made available through the WHOIS service, should be responsible for keeping the database accurate.¹⁵

Both the U.S. Government's White Paper¹⁶ and the subsequent implementation of its recommendations in ICANN's RAA hold registrars accountable for the collection, provision, and maintenance of registrant information. The penalty for failure by the registrant to provide accurate registrant information is the cancellation of the domain name by the registrar. The penalty for failure by the registrar to satisfy the requirements in the RAA is cancellation of accreditation.

As explained earlier, according to ICANN's RAA, accredited registrars are obligated to collect, maintain, and furnish to the public contact information for SLD registrants. Section II.J.8 provides that a

registrar shall abide by any ICANN-adopted policies requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with an SLD registration . . . or (b) periodic re-verification of such information . . . In the event [a] registrar learns of inaccurate contact information associated with an SLD registration it sponsors, it shall take reasonable steps to correct that inaccuracy.

The IACC believes that failure by a registrar to take steps to verify and re-verify contact information should be considered a breach of the RAA. According to Section II.N, “[the RAA] may be terminated before its expiration by ICANN in any of the following circumstances: . . . 4. Registrar fails to cure any breach of the Agreement within fifteen working days after ICANN gives Registrar notice of the breach. To the IACC's knowledge, there have been no such actions taken by ICANN, despite widespread complaints regarding the inaccuracy of WHOIS information.

¹⁵The IACC's statements apply to the obligations accepted by ICANN-accredited registrars of generic top-level domains (gTLDs). Obviously, much less control can be exerted over the data-related practices of registrars who are either unaccredited, register only country code TLDs, or who are part of a movement to create an alternative to the DNS. These “alternative roots”—top level domains which have been created outside the ICANN-recognized “root server” system. Most of aggressively marketed alternative—new.net—now claims to be accessible to over 40 million U.S. Internet users. Some of these alternatives—including new.net—make some WHOIS data available to the public, but none are subject to ICANN requirements in this area, and all create a serious risk of consumer confusion.

¹⁶63 Fed.Reg. 31741, 31750 (June 10, 1998): “Trademark holders and domain name registrants, and others should have access to searchable databases of registered domain names that provide information necessary to contact a domain name registrant.”

ICANN's capacity to enforce the WHOIS obligations contained in the RAA needs improvement. For instance, despite the public statement by the General Counsel of ICANN that "most registrars appear not to be in compliance" with their RAA obligation to provide a fully searchable WHOIS,¹⁷ the IACC is not aware of any enforcement action, formal or informal, that ICANN has ever taken to enforce this obligation. This is particularly disappointing in light of ICANN's strongly expressed view that only it, and not any third party, can enforce the WHOIS-related obligations of an accredited registrar under the RAA.¹⁸

Accredited registrars also have some obligations under the RAA concerning WHOIS data quality. The prevalence of inaccurate or outdated contact information in the WHOIS database limits its usefulness as an anti-piracy tool. The RAA gives ICANN the authority to develop data quality or verification standards that registrars would be obligated to fulfill. ICANN has not done so, even though steps could easily be taken to eliminate obviously false contact data at little or no cost to registrars. The RAA also requires registrars to accept reports from third parties (such as intellectual property owners) of false contact data, and to cancel registrations when contact data cannot be verified. Compliance with these obligations is extremely sparse.

The U.S. government should urge ICANN to pay more attention to the implementation and enforcement of the registrars' RAA obligations and to increase its efforts to restore WHOIS at least to the level of usability that the public enjoyed up until the advent of registrar competition in 1999. Since the gTLD WHOIS environment provides a template for these services in other parts of the DNS, increased attention here could improve accountability and transparency throughout the Internet.

In addition to better enforcement of existing obligations, ICANN must direct its accredited registrars in developing a method for ensuring that the information collected upon registration and renewal is accurate. One suggestion would be to use the credit card holder's information as the registrant contact information in the WHOIS database. If websites selling books or clothing do not process transactions unless the mailing address and billing address are the same, why shouldn't an SLD registrar be required to confirm that information?

Bringing greater transparency and accountability to the gTLD and ccTLD world through improved public accessibility of registrant contact data must be a high priority both for ICANN and for the U.S. government. In its participation in ICANN's Governmental Advisory Committee (GAC), the U.S. should continue to urge its foreign counterparts to insist that the operators of provide free, real-time, unrestricted public access to the full range of WHOIS data elements. Such a step would be in the best interests of consumers, creators, and Internet users in each of these countries, and would facilitate the full integration of these ccTLDs into the mainstream of global electronic commerce. The U.S. government should also ensure that the ccTLD, which it controls, .us, provides a model in this regard. Finally, we need to consider what steps should be taken to ensure that U.S.-based "virtual gTLDs" that operate two-character domains that have been delegated to them by foreign territories adhere to the best possible practices with regard to transparency and accountability, lest they become havens for online piracy and an embarrassment to the United States.

Conclusion

The IACC urges this Committee to continue its support for an open, accessible and accurate WHOIS database. IP rights and privacy interests are not mutually exclusive level of transparency and accountability required by our laws. The IACC recommends the following steps as concrete actions that would improve WHOIS and provide mechanisms for protecting consumers and IP owners.

1. WHOIS database operation must continue to be mandatory for all ICANN accredited registrars, regardless of the gTLD the registrar is managing;
2. Registrars must obtain, and maintain basic contact information;
3. The information must be publicly accessible;
4. The information must be verifiable; and
5. The information must be kept up-to-date.

Thank you again for this opportunity to provide these comments on behalf of the IACC's member companies. I would be happy to answer any questions.

¹⁷ See <http://www.icann.org/committees/WHOIS/touton-letter-01dec00.htm>, question 7.

¹⁸ See to ICANN's amicus filing in *Register.com v. Verio*, posted at <http://www.icann.org/registrars/register.com-verio/amicus-22sep00.htm>.

Mr. COBLE. Thank you, Mr. Trainer.
Ms. Fena?

**STATEMENT OF LORI FENA, CHAIRMAN OF THE BOARD,
TRUSTe**

Ms. FENA. Thank you, Mr. Chairman. I appreciate the opportunity to testify for the Committee.

I'm here today as chairman and co-founder of TRUSTe, the organization which is a nonprofit organization focused on protecting individuals' privacy rights in the networked world and respecting individual—the balance of individual information together with the business interest.

We're most known for our privacy seal program, which is the largest seal program to date. We cover 7 out of 10 of the most trafficked sites, I believe 50 out of 100 of the top trafficked sites; and according to Cheskin Research study of trust in the networked Americas, we are the most trusted, recognized symbol.

We found in this process that we are here today to not only talk about how we use the Whois Database for enforcement purposes to protect privacy, we also have—are here to testify about how the fair information practices which are essentially the basis for our TRUSTe seal program in the online world for websites is actually something that we feel would be very applicable in looking at how the Whois Database is managed to make sure—we found that using the same type of capability or business infrastructure for the Whois Database, making sure that people know what information is being collected, for what purposes, with whom it will be shared with, and making an enforcement and accountability a major part of the process will great increase not only the consumer trust and accuracy, it will incredibly increase the accuracy of the information. We've found this to be consistent with the implementation of the TRUSTe program online.

We use a contract, and we use contract law, since the privacy laws across the U.S. are not—the privacy laws globally are not harmonized. We use contract law for enforcement very much like the intellectual property laws to enforce this. But what we've found in enforcing privacy is you can, in fact, use the systems and infrastructures of fair information practices to enable companies and individuals to balance this trust.

I'd like to just move forward and say that although there's a great need to allow consumers—intellectual property owners to move around and have access to this database, we've also found it's extremely important because in the online world it's not just companies that are trying to figure out who is behind a database. It's—or who is behind a website. It's also something that's publicly available to consumers, and consumers can actually go to a Whois Database and find out and take individual action to find out or to notify different companies, not just individuals but different companies that are infringing on their rights.

So we feel that access and availability of the Whois Database is extremely important, not only for intellectual property right holders' enforcement of privacy but also to build a system of accountability and trust. And that kind of transparency is something that will create a trusted network globally. So we feel that the access

and accountability will actually increase accuracy, and we would like to have fair information practices that are currently being used and implemented in the online world be adopted by the registrar system as well.

Thank you.

[The prepared statement of Ms. Fena follows:]

PREPARED STATEMENT OF LORI FENA

Mr. Chairman and Members of the Subcommittee:

My name is Lori Fena. I am the Co-Founder and Chairman of the Board of Directors for TRUSTe. I would like to thank you for the invitation to testify today about TRUSTe's experience with the WHOIS database.

As many of you know, TRUSTe is a non-profit organization dedicated to enabling individuals and organizations to establish trusting online relationships based on respect for personal identity and information. Four years ago, we created the TRUSTe Privacy Seal Program to serve as a guidepost for consumers so that they could safely navigate the Internet.

Under our seal program, Web sites must abide by a set of fair information privacy practices developed by the private sector and endorsed by the Federal Trade Commission (FTC) and the Department of Commerce. Organizations that participate in our program also agree to abide by TRUSTe's Watchdog dispute resolution mechanism in which consumers can turn to TRUSTe to resolve their privacy related disputes.

The backbone of the TRUSTe program is the legally binding contract that each Web site must sign with us. This contract gives TRUSTe the power to ensure that companies abide by their posted privacy statements.

Today TRUSTe:

- Maintains the largest privacy seal program with more than 2,000 Web sites world-wide that have met our rigorous certification process.
- Oversees the privacy practices of 8 of the top 10 Web properties, all of the Internet portal sites, and 50 of the top 100 most trafficked Web sites.
- Acts as an FTC-approved Children's Online Privacy Protection Act (COPPA) Safe Harbor.
- Was the first organization to join the Department of Commerce's European Union (EU) safe harbor.
- Provides verification and dispute resolution for the EU safe harbor.
- Maintains the most prominent symbol on the Web for nearly two years according to an ongoing survey by the measurement firm Nielson/NetRatings.
- Resolved over 1,200 consumer disputes in 2000 alone.

Research indicates that privacy, accountability, and transparency increase trust on the Internet. A recent study by Cheskin Research identified the TRUSTe Privacy Seal as the most trust-invoking symbol online. In its survey entitled "Trust in the Wired Americas," Cheskin indicated that more than half of the respondents (55 %) displayed higher levels of trust in a site that posted the TRUSTe Privacy Seal.

Research like this demonstrates two key points. First, consumers have come to rely on the TRUSTe Privacy Seal as a guidepost in determining which sites deserve their business and, more importantly, which do not. Secondly, businesses will voluntarily subject themselves to the fair information principles, third party oversight, and dispute resolution because it helps them build trust. Simply put, the business community understands that good privacy is good business.

Therefore you can understand why maintaining the integrity of our privacy seal is paramount to the general public's privacy protection and safety on the Web.

I am testifying today, Mr. Chairman, not as an expert on the WHOIS databases; rather, I am here to deliver a case study of how the WHOIS database has helped our efforts to ensure that consumers find only legitimate TRUSTe seals. Based on our experience implementing and enforcing the fair information practices over the last four years, I am also here to discuss how these practices can be used in the WHOIS database to create a system of trust, accountability, and accuracy.

It is within the context of building a safe Web community and protecting privacy that TRUSTe uses the WHOIS database. From the beginning, TRUSTe anticipated that some companies would seek to take advantage of consumers by falsely alleging participation in our program. Therefore, we have taken precautions to safeguard against the inappropriate use of our privacy seal.

On a regular basis TRUSTe depends upon the information provided in the WHOIS database to find and contact Web sites that are illegally or improperly posting the TRUSTe seals. When information about a Web site owner is accurate and accessible, TRUSTe can contact offenders and arrive at a speedy resolution.

However, there are a few sites that illegally display our seal and, not surprisingly, do not post accurate contact information on their Web site. It is these fly-by-night operations that create the need to balance the privacy rights of the Web site owner with the safety of the public at-large.

As one example, last October, Americanpolitics.com posted our privacy seal, thereby claiming to participate in our oversight program. It was only after we used the WHOIS database to find the Web site owner that we were able to get the site to remove the illegally posted TRUSTe privacy seal.

In this way, the WHOIS database has been and continues to be instrumental in enabling TRUSTe to have fraudulent TRUSTe privacy seals removed from Web sites.

Consumers also use the WHOIS database as a resource for determining where a company is located and how to contact them. Accurate contact information from a reliable source provides consumers with the assurance that the company can be held accountable and gives them the means for pursuing recourse.

In order for this database to be efficient and effective for both consumers and businesses, the public information needs to be accurate and accessible. By following the fair information practices of notice, choice, access and security, the WHOIS database can balance the safety of the public at-large with the privacy of Web site owners.

As it stands today an accredited domain name registrar is not required to allow domain name registrants to opt-out of having their personal information provided to third parties for marketing purposes. This type of an opt-out should be provided to all registrants.

The information in the WHOIS database needs to remain public for the benefits it provides to consumers, individuals and businesses of the Web community. However, individuals and companies registering their domain need to clearly know how this information will be used and how to control it. Providing the database information to mass marketers without providing those in the database even the courtesy of allowing them to opt-out does not create a trusting, transparent and accountable system. This is even more true when there is little practical alternative for those registering. Indeed, some individuals or companies may choose deliberately to falsify their information, since it may be the only effective way to avoid receiving unwanted marketing material.

Clearly, the WHOIS database has been an important tool for consumer safety and, in our experience, has been an irreplaceable means of ensuring the validity of the privacy promises that companies make. This will become even more important moving forward.

In conclusion, we feel the WHOIS database is an important aspect of privacy and accountability in a networked world. It would benefit the system greatly to implement the fair information practices.

Mr. Chairman, I appreciate the invitation to testify here today, and will be happy to answer any questions you may have.

Thank you.

Mr. COBLE. Thank you, Ms. Fena.

Dr. Catlett?

**STATEMENT OF JASON CATLETT, PH.D., PRESIDENT AND
CHIEF EXECUTIVE OFFICER, JUNKBUSTERS CORPORATION**

Mr. CATLETT. Thank you, sir. It's an honor to appear before you, and I thank you for the invitation.

Mr. COBLE. Pull that a little closer to you, if you would, Doctor, to activate your—

Mr. CATLETT. If you're looking to me for controversy, I'm afraid you won't find it on the topic of intellectual property. I'm a U.S. patent holder. My company has a trademark. It owns and is a software publisher itself. The importance of intellectual property rights is something that I'm thoroughly supportive of.

I'm also—

Mr. COBLE. If you'll suspend, Doctor, when I used the word "controversy," maybe I should have said "disagreeing agreeably." That could have been perhaps a more sanitized version.

Mr. CATLETT. I will find something to disagree on. Thank you, Mr. Chairman.

The issue of accountability is also important to me. In my fights against spam—as I have personally received death threats, my website has been subjected to denial-of-service attacks, attempting to prevent its continued operation. So—and in my fight against spam, as I've become very familiar with the question of where the balance between anonymity on the Internet and accountability for actions should be placed.

Now, in the case of spamming, it's certainly true that in some cases spammers can be found by simply looking up their entries on the Whois Database. Unfortunately, this is the more incompetent form of spammer that you will usually find by this process, the one that didn't really bother to try and conceal their criminal intentions.

In talking with experienced fighters against spam with consumer protection officials, we find that the Whois Database is really not terribly useful because of exactly the reason that Mr. Berman raised, that many of the entries are Mr. Evil Angel of a fake address. Or even if the address is plausible, then it turns out to be not by the person that it claimed to be. So the idea that the self-reported information in the Whois Database is an effective one for tracing criminal activity is mistaken.

What is more reliable in the experience of anti-spammers is to go to the actual publication, the point of publication. Merely having a domain name doesn't enable you to publish anything. You have to get an ISP. You have to be connected to a computer. And it's possible to use both technical means and also administrative procedures to get to the point of publication, which is what matters to the copyright infringement.

Now, we could ask, What is the proper degree of anonymity that people should be able to have on the Internet? I think there should be some right to anonymous speech on the Internet. As Mr. Berman—as you mentioned, political speech deserves protection here. But ultimately there has to be some accountability.

Should that accountability be in the form of mandating the provision of the information available to anybody to download from the database? I think that's inconsistent with our experience in other technologies. If you look, for example, at a driver's license, can you look up the driver's license of someone in the car park when you get home on the Internet and find his home address? No. Congress has properly moved to protect the privacy of drivers with the Drivers' Privacy Protection act.

Now, there are still procedures by which, if, for example, you've been run over by a driver, you can trace back those people. And analogous procedures should, in my opinion, be available for domain name information. It should be possible to find and revoke that domain name if necessary. However, making the information public for all comers is a gross overkill.

I have three specific recommendations today. To assist in the lessening of unwanted solicitations by junk e-mail, it would be

greatly helpful if ICANN were to mandate an additional field in the database whereby the holder of a domain name can elect to say I want to receive spam or I don't want to receive spam or that they haven't made any such election. This would have no impact on any of the intellectual property issues that we've had here today, but it could be very useful for the statutes of California and possibly future federal legislation.

My second recommendation is that domain name owners should have the option to have their contact information withheld from the public database and rely on a procedure by which some aggrieved party can obtain that with appropriate contractual controls.

The third one is that ICANN should look at the possibility of pseudonymous registrations whereby they do not have to give the information to the registrar themselves. Now, that also would have to be the subject of a consideration for these accountability issues, but I think it's an important one to do.

So I thank you very much for your time today.

[The prepared statement of Mr. Catlett follows:]

PREPARED STATEMENT OF DR. JASON CATLETT

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp. I'm grateful for this opportunity to speak here today.

Junkbusters is a for-profit company whose mission is to free people from unwanted commercial solicitations through media such as email, physical mail, telephone, and faxes. (The Whois database is a major source for contact information for all these media.) Since our web site launched in 1996, millions of people have turned to us as a free source for information, services and software for stopping junk messages, particularly email. I have assisted many government organizations and legislators on email and other privacy issues since the Federal Trade Commission asked me to explain the mechanics of spamming at their public workshop on the topic in 1997.

I commend the committee for holding this much-needed oversight hearing on the Privacy and Intellectual Property Issues of the Whois Database. I have little to contribute on the topic of intellectual property, other than to say that it is in a sense somewhat irrelevant to the privacy interests of an individual whether an organization owns a item of personal information about a "data subject" (as privacy lawyers call the individual concerned), versus whether the organization buys, licenses, barter, scavenges, or steals the data from another party. These are essentially commercial considerations. The key privacy questions are whether the data subject consented to the collection, disclosure and use of the data, whether the organization handles the data fairly and lawfully, and what rights of redress the data subject has if it does not.

PRIVACY

Definitions of privacy generally fall into one of two types, both of which are acutely relevant here. The first is "seclusion from intrusion," or the "right to be let alone," to use the phrase made famous in the 1890 law journal article by Brandeis. The second is "informational self-determination," the right to control the collection, disclosure and use of information about oneself, formulated by Alan Westin in his 1967 book "Privacy and Freedom" and now the basis of most modern privacy statutes worldwide. To take obvious examples in context of the Whois database, the first definition addresses whether an individual registering a domain receives spam or unwanted solicitations via other media, and the second includes whether information is gathered or sold by other parties about the registrant without her knowledge and consent.

Violations of these two types of privacy tend to be correlated, since the gathering of contact information is a means towards the delivery of an unwanted solicitation, and because the targeting of messages based on further information makes the activity more economically attractive. As an illustration, the San Francisco Chronicle reported in 1997 that Barnes and Noble, an online bookseller, had established software systems to search people's home pages for references to certain authors, and emailed them solicitations to purchase new titles in the genres mentioned. Inde-

pendent of the fact that the company should have known better than to try spamming (and soon discontinued the practice), many people were disturbed by the idea that a profile of their reading tastes was being assembled in this robotic manner by an unknown party, let alone being confronted with personalized recommendations based on them. Even fans of book catalogs might be unsettled by a physical letter beginning “Dear Murder Enthusiast” or detailing some interest that they intended to share only with a few friends. Given that the compilers of marketing lists have for years used Whois registration information as a source of personal information (in some cases scavenged free, in others bought from registrars), concerns over the data privacy are well justified. Most people avoid putting their home address on their web sites, and they should be able to register a domain name without effectively giving up this precaution.

The public policy objective of privacy law is to preserve the individual’s right to privacy, while still permitting societal participation. This is somewhat analogous to intellectual property law, which seeks to encourage the publication of products of the intellect by providing certain rights to inventors and authors to control the subsequent distribution and use of their work. The current situation with the Whois database is unsatisfactory because individuals are effectively required to sacrifice some of their privacy in order to participate in a fundamental Internet activity. Courts have remarked that the Internet has provided an unprecedented opportunity for free speech; participation should not be dampened by avoidable erosions of privacy.

The current (1999) ICANN Registrar Accreditation Agreement does contain some provisions relating to privacy, but they are inadequate in both theory and practice. [See <http://www.icann.org/nsi/icann-raa-04nov99.htm> at J.7.a and F.6.f] The agreement anticipates the possibility of a registrant licensing a domain to another party whose contact details are not disclosed, but this is not a satisfactory way of preventing disclosure for the average user. The agreement also requires the registrar to impose an undertaking not to use the email addresses from the Whois database for sending Unsolicited Commercial Email (UCE, or spam), but in practice this is ineffective. Spam is discussed further below, and my statement here concludes with a set of specific recommendations for ICANN. Mine is not the only privacy organization to seek such reforms; see for example the Electronic Privacy Information Center’s letter of February 16 to Congressional Privacy Caucus on this topic. [<http://www.epic.org/privacy/internet/ICANN—privacy.html>]

The requirement of the publication of registration information can be seen as egregious and anomalous when compared to analogous media. Telephone subscribers are universally given the option of a non-published (unlisted) number, regardless of which local phone company they use. The US Postal Service discloses information about the identity of a post office box holder only if the holder solicits funds from the public. Various statutory privacy rights have been established to protect the nexus of contact in different media, such as the prohibition in California against telemarketing calls to non-published numbers, so-called “asterisk laws” in several states mandating an optional designation in directories for published numbers that must not be telemarketed, the federal prohibition against junk faxes, and the opportunity to issue prohibitory orders against senders of unwanted solicitations via US mail. This procedure was upheld by the Supreme Court in 1971, including its restriction on the subsequent sale of the address in marketing lists. My first recommendation below is an addition to the Whois database to support this kind of protection for email addresses.

Given the lack of such protections in the online world, plus the ease with which contact information may be inexpensively gathered, it is hardly surprising that surveys routinely find privacy is the number one concern of Internet users and a major reason for non-participation by the offline half of the population. The basic operation of establishing a homestead in cyberspace should not stand as an example of the lack of respect for privacy in the architecture of the Internet, particularly when a few appropriate curtains could be added with comparatively little effort. To be fair to the original architects, many of their procedures were devised at a time when the individuals involved were few and often known personally to one another, so it is understandable that privacy does not appear to have been a top design priority. Changes are now overdue.

ACCOUNTABILITY

Privacy is a fundamental human right, but it is not an absolute right: it should not provide impervious and permanent cover for criminal activity, for example. Appropriate mechanisms should be in place for personally identifying disclosures in the case of law enforcement investigations, and for civil litigation such as libel, trade-

mark and copyright disputes. But these mechanisms should restrict disclosures to what is necessary and fair; checks and balances should protect against misuse. Making contact information available to everyone is as much an overkill as if a DMV were to require people to display their drivers licenses on their lapels when standing on the sidewalk.

Domain names do somewhat differ from other media in that they enable the registrant to establish an identity that can be used in the role of a publisher as well as a subscriber to a multi-way communications channel (though fax broadcasting has a similar quality). But the actual publication is typically performed by an Internet Service Provider, or at least via an ISP, and ISPs do not generally require the public disclosure of contact information for the source. Why should registrars be any different? ISPs are accustomed to tearing down web pages or providing subscriber information when required to do so by a court order. The same procedures can apply to domain name registrations if this additional step is needed.

SPAMMING

The problem of spamming is one of the most important and instructive topics for analysis here. Spamming is not a criminal offense in most states, but it is socially damaging, undermines consumer confidence in the Internet, imposes on consumers and businesses billions of dollars in wasted costs annually, and violates the terms of service of ISPs. As I have said in testimony before the Senate, I believe spamming should be prohibited by federal law, and perhaps it will be. But even if it is, people should still be able to try to avoid spam by reducing the exposure of their email addresses, and those who are harassed by spammers should have the means to obtain redress, which in practical terms translates into identifying the spammer.

The most obvious damage to privacy from the Whois database is due to the so-called "harvesting" of email contact addresses by spammers. (I prefer the term "scavenging" because the crop being reaped was not planted by the scavenger.) As mentioned above, the ICANN agreement with registrars requires the registrar to impose an undertaking not to use the data obtained to facilitate spamming. Unfortunately spammers can blithely ignore the "you agree not to" message attached to the responses to their requests, because their access is essentially anonymous. Limits are often placed on the rate at which domain name queries are answered from any given IP address, but this merely reduces the speed with which the addresses are obtained, and is ineffective in the long term. It cannot prevent scavenging any more than a supermarket could prevent shoplifting by limiting the numbers of bags shoppers are allowed to carry out of the store.

The observation has often been made that Whois contact information can help track down spammers, and I certainly agree that this is sometimes the case. Unfortunately it is rarely much help against career spammers, who have registered large numbers of domains with contact addresses such as the Martian embassy and phone numbers such as 202-555-1212. Beyond these patently false addresses lie more plausible but incorrect entries. Experienced spam hunters tend not to rely on such self-reported, unauthenticated and too-often inaccurate information; rather they examine the header information on the email and use software utilities such as "traceroute" to establish the ISP that originally carried the spam, and then ask the ISP to terminate the account. The casual spammer will usually desist after a warning from his ISP. Furthermore, almost all spammers give other generally more reliable clues to their identity in the content of their emails, which are seldom abstract messages such as "Sin no more." They often ask the addressee to visit a particular web site, which can be tracked via traceroute and the hosting ISP, or in the case of a site accepting credit card payment, through the banking system. Many spams ask directly for checks to be sent to a post office box specified in the email, which can also be followed. In practice, self-reported contact information is like a weak door lock that keeps out the honest unintentional intruder while presenting no serious challenge to the dedicated burglar. I do not believe the benefits of tracking amateur spammers via the self-reported contact details from the Whois database outweigh the damage to privacy caused by the public availability of the information.

REDUCING PERSONALLY IDENTIFIABLE INFORMATION

Various other benefits of contact details being public have been cited, but none of them persuades me that administrative contact must be made public. Technical contact information is certainly useful for maintenance tasks, but most technical contacts are business-title roles at ISPs, not individual registrants. The fact that consumers find it useful to authenticate a business using the administrative contact information from the Whois database is no reason to require it of all registrants, any more than residential phone subscribers should be forced to have yellow pages

entries. Businesses that consider it beneficial can elect to do so, as proposed in my second recommendation below.

ICANN states in the preamble to its June 2001 survey that more than 70% of its registrations are by organizations. [See <http://www.icann.org/dns/whois-survey-en-10jun01.htm> under Background] The remaining twenty-something percent still adds up to a very large number of individuals whose privacy is being compromised by their registrations. A policy question arises whether organizations should be treated differently to individuals. Only natural persons have privacy rights; entities such as corporations do not, though they may have an interest in confidentiality: considerable public speculation has arisen from domain names registered by large companies such as Amazon and Microsoft. In the case of sole proprietors, the entity may appear to be an institution when it is in many ways more like an individual. For these reasons it seems to me appropriate to give institutional registrations exactly the same control over admin and billing contact information as individuals have for personal registrations.

I further believe that it may be desirable and feasible for domain names to be registered with a pseudonym (such as a registrar-issued customer number), so that no personally identifiable information is provided, not even to the registrar to whom payment was made (presumably with a money order). Anonymity and pseudonymity are the most reliable ways to protect privacy: there is no possibility of personal data being disclosed or used inappropriately, because it does not exist. (The difference between anonymous and pseudonymous speech is that while neither is identified as originating from a specific individual, the pseudonym allows continuity of interaction and attribution.)

If participation in the digital network without identification raises concerns in your minds about accountability, consider how routinely this occurs on the telephone network: with a payphone, using a popular privacy-enhancing technology called coins. Doubtless some crimes are facilitated by this opportunity, but nobody would consider this as a justification for retrofitting the nation's payphones with credit card readers or for abolishing the quarter. In some countries, including Italy, it is even possible to subscribe to a prepaid mobile telephone service without identifying oneself to either the carrier or the government. If the phone appears to be involved in criminal activity, law enforcement can have the service suspended or obtain the identity of subscriber by examining the numbers called or by wiretapping calls. The situation for pseudonymous domain names would be analogous.

Notice that the registration itself is unlikely to be considered criminal: even if the text of the domain name were arguably libelous or blasphemous, is there any prospect of real harm merely from its presence in the Whois database? Registrars have already addressed the question of obscene domain names, and can decline to register them if they consider them offensive. Even in the case of trademarks, it is far from clear that merely registering FamousNameSucks.org without publishing a corresponding web site would constitute infringement. Rather, it is activities other than registration that constitute the wrongdoing, and those activities entail their own means of tracing the malefactor: the Whois database cannot reasonably be expected to serve that purpose, any more than the white pages should be expected to deter harassing phone calls.

Where it is found appropriate to revoke a domain name, it is obviously just as easy to terminate domain name service for a pseudonymous account as it is for one registered to Thomas Paine or the Federalist Publishing Company. The Famous Name Corporation can still sue a John Doe defendant, seek his identity from an ISP, and persuade a court to have the registration transferred to it.

If a Unabomber wishes to publish his manifesto anonymously, he is likely to find other options preferable to registering the domain ExplodeTechnologists.org. Even if he did wish to establish such a web site, he would be more likely to give his administrative contact address as Mauritius rather than Montana. The FBI would be no more hampered by pseudonymous registration than the false details in this registration; its agents would probably sooner seek the assistance of the ISP hosting the domain rather than sending field agents to the Indian Ocean. Some spammers favor disposable return email addresses, which pseudonymous registrations could provide, but they are already have that by claiming to be from the Martian embassy, or less flagrant false addresses. Also, free web-based email services have a cost advantage to the spammer over domain name registration. In short, pseudonymous registration of domain names seems unlikely to lower the practical level of accountability for objectionable behavior, because such behavior can more reliably and appropriately traced by other means.

Pseudonymous registration does raise some logistic questions, such as how renewal notices are to be sent (perhaps by anonymous remailers), but I believe that

deliberation would likely find practicable solutions, so I suggest that ICANN investigate the question.

This is one of the following several specific recommendations I respectfully submit to ICANN and the committee to improve the privacy of registrants and Internet users.

RECOMMENDATIONS

1) UCE field: The addition to the registration database of a field indicating the registrant's disposition towards Unsolicited Commercial Email from any party to email addresses within the domain (not merely the one provided as part of the registration). At least three possible registrant responses should be supported: unwilling, willing, and not indicated.

This measure has similarities to the "do-not-call" lists and "asterisk laws" that several states have passed against telemarketers. The UCE field may be usable under existing state anti-spam legislation such as California's, and possibly by future federal and state legislation. 2) Disclosure election: Registrants should be given the opportunity to indicate their disposition toward disclosure by their registrar of billing and admin contact information. At least three possible registrant responses should be supported: unwilling, desired, and not indicated.

I believe ICANN should require this of registrars. This option should apply not merely to email address, but to all contact data. Domain name registrants receive a great deal of junk physical mail as a result of registering (some due to their registrar actively selling the contact details as a mailing list). Registrants should not have to be burdened with this.

In the case of Registrars who wish to sell for marketing purposes contact information about their registrants (versus distributing it via the Whois database), separate affirmative consent should be required (opt-in).

3) Population of fields: A program to encourage or require registrars to seek and process customers' elections for the above two fields (UCE and disclosure).

Registrants need not be immediately pestered for a response, but the process should be easily available via the registrar's web site, and the question should be posed prominently at the time of renewal. Consideration should be given to whether the registrant's response ought to be made public as part of the Whois database; this transparency may be beneficial in seeing whether registrars are withholding or providing data about registrants who have made no election.

4) Plaintiff's procedures: The development of standard procedures for the processing by registrars of requests for the on-forwarding of messages to, or the disclosure of contact information about, registrants who have elected against disclosure of their contact information.

A typical question here is what should happen when a trademark owner wishes to send a cease-and-desist notice to the operator of a web site. The procedure should not impose undue burdens or liability on registrars.

5) Development of appropriate legal mechanisms to support the three points above.

Privacy rights require an enforcement mechanism with a sound legal basis. For example, if a registrar discloses a registrant's personal data contrary to her instructions, what procedures does she have for redress?

6) Pseudonymous registration: The development of appropriate mechanisms to support pseudonymous registrations.

I believe that the steps I recommend above would greatly improve the privacy of Internet participants without significant deleterious side-effects.

I appreciate the opportunity to speak with you today. I would be pleased to answer your questions.

Mr. COBLE. Thank you to each panelist. Let me start, Ms. Fena, with you, if you would elaborate on some of the problems that you have encountered with the infringement of your trademark and logo on the Web, and let me put a two-part question to you. Are there cases where you see a violation and cannot pursue legal recourse due to inaccurate or faulty Whois information, A? And, B, in those cases, are there any Government authorities, such as the FTC or the Department of Justice, upon whom you could call for assistance?

Ms. FENA. Thank you, Mr. Chairman. Yes, as a matter of fact, in policing our seal, we do have a contract with the sites that legiti-

mately post our seal, and we can usually enforce those quite well. The issue comes up when somebody misappropriates our seal and posts it. We have technology that goes out and verifies seals that are out there, and every now and then, technology will run across a seal that is not something that we granted, and they are illegally posting the seal and hoodwinking consumers.

In those cases, we have, in fact—an example would be americanpolitics.com. Last year, in the year 2000, we went to the Whois Database and found information about the site, but frequently, when we go to the Whois Database and the information is inaccurate—as you mentioned, 1234 Evil Avenue—we also have run into situations where most of the hoodwinking types of companies that would misappropriate our seal are also the companies that would provide misinformation to the Whois registrar—to the Whois Database in their registration.

In those cases, we can then move on to hopefully working with the ISP in a cooperative manner to be able to access who is—you know, who is paying them for serving up that site. And sometimes that becomes a black hole because you can actually prepay or you could use an illegal, you know, credit card to do that.

So there is a chain that you can go through, and frequently, when that doesn't work, we would end up stepping in to, you know, talk with governmental enforcement agencies such as the FTC. Frequently, when we can't enforce the four corners of our contract in contract law, that is what we do. We step to partner with the Government in doing that.

Thank you.

Mr. COBLE. Thank you.

Mr. Trainer and Mr. Mitchell, you all referred in your testimony to instances of criminal prosecutions for intellectual property violations. Give us, if you can, an estimate as to the dollar value of the losses involved in those circumstances and whether the Whois information assisted or helped to minimize the damages.

We'll start with you, Mr. Mitchell.

Mr. MITCHELL. Yes, thank you, Mr. Chairman. I would appreciate an opportunity to follow up in writing to document that more specifically.

Mr. COBLE. That will be—without objection, that'll be fine.

Mr. MITCHELL. We are actually involved in a number of procedures now to seek restitution on behalf of our members and to more accurately calculate those sorts of losses. I can assure you, however, that in those investigations, Whois did play a crucial part in finding the source of the infringement, shutting it down, and reducing the resulting damage.

Mr. COBLE. Mr. Trainer?

Mr. TRAINER. Mr. Chairman, I know that I don't have the exact figures that you're requesting. We do have members, though, that I can tell you that maintain in-house capacity just to go after people who are violating their intellectual property online, and they often find problems with the Whois Database. One example that I got just late yesterday was one of our member companies tried to do a Whois search and finding this person named Sal Menella, which may sound like a real problem you would have otherwise, but Sal Menella resides in a place called Hickville, Kentucky. So

this is a concrete example of completely false information. They couldn't go after this person. So obviously it requires more resources to track down people when they're offering links to pirate—pirate CDs and other things.

But as far as a dollar figure, at this particular point I don't have that.

Mr. COBLE. Okay. If you could give us an approximate amount, and, Mr. Mitchell, you as well.

Now, I have a couple more questions, but my 5 minutes will expire. So I'm going to recognize the gentleman from California, and I'll come back for a second round. Mr. Berman?

Mr. BERMAN. I'd like to ask Dr. Catlett a couple of questions. In your testimony, you support necessary and fair disclosure of domain name registration information—

Mr. CATLETT. Absolutely.

Mr. BERMAN [continuing]. For civil litigation, such as libel, trademark, and copyright disputes.

Mr. CATLETT. Yes.

Mr. BERMAN. Could you elaborate on what you think such necessary and fair disclosures would be? Should trademark and copyright holders be allowed to freely peruse Whois information? Do you believe it is necessary and fair to place limits on mere access to Whois information? And if so, what limits?

Mr. CATLETT. Well, I think the procedure should restrict the use of the information to an appropriate purpose. For example, if a company were to come in and request a lot of information about domain name holders under the pretext of an infringement investigation, it shouldn't be able to use that information for marketing. There should be—

Mr. BERMAN. Shouldn't be able to use that information for marketing?

Mr. CATLETT. Should not be able to use that information for marketing purposes to try to sell something. A well-known principle in privacy law states that information should be collected for a specified purpose.

Mr. BERMAN. How would you deal with the proof problems in that area? Going in—access to information because you had a legitimate purpose, then having the information and using it for the non-legitimate purpose?

Mr. CATLETT. Well, I think it would come out if the company were doing that, that this had happened, people would get junk mail, for example. The quantity would show. I think that it would become evident that that had happened, and such an act could be penalized by not being allowed further use of the information.

I think it's very unlikely that a large-scale violation of that type would continue.

Mr. BERMAN. Say the last thing you said again.

Mr. CATLETT. I think—I think it's very unlikely that a large-scale violation—scenario of that kind would continue. But the principle should be there to say companies should not be able to use for marketing purposes information gathered under—under an investigation of copyright infringement.

Mr. BERMAN. What do Messrs. Mitchell and Trainer think of that idea, requiring access for, at least in one case, pursuing investiga-

tions of IP violations and—but making a prohibited activity the shifting of the use of the information for these other purposes?

Mr. MITCHELL. Thank you. We believe that an approach like that, however satisfactorily it may allow for intellectual property-related investigations, would deny a number of significant other uses of the Whois Database to parents, to consumers. It would take away a significant tool that anyone looking to engage in commerce on the Internet currently has to check out the reliability of someone they are planning on engaging in business with.

We have a number of cues in the physical world to determine whether we want to pursue a business or a personal relationship with someone, whether the business continues to be there day after day, whether it carries a reputable brand name on its sign out front, its on-hand inventory, the fact that the check-out folks are people we see and we know and recognize. None of those cues are available to us in making fundamental decisions about whether to engage in commerce or leave private information with a site that's on the Internet. Whois provides one of the few links to real live people behind the website, behind the URL.

Mr. BERMAN. You know, the irony is I've spent some time—we've spent some time critical of ICANN for not pushing these new registries or conditioning approval of these new registries in the disclosing—in the requirement to disclose adequate information about people who want to run websites and get domain names, and also about the total weaknesses in many of the registries' operations in verifying. But now I listen to the folks who were representing people who had come to us about these problems, and you seem to be saying everything's pretty good right now, just leave it the way it is, even as you acknowledge—or at least don't—at least some have said on the panel the verification problem, the accuracy problem is quite serious and these people have a very inadequate database of information.

Mr. MITCHELL. We are satisfied with our current level of access to many of the generic top-level domain Whois Databases. They allow us not only to identify—

Mr. BERMAN. Many, but not all.

Mr. MITCHELL. Right. That's correct. We believe that improvements can be made in virtually all of them and are pursuing negotiations one on one with the registrars themselves.

We are concerned about data quality, as you recognize, and believe that improvements can be made there, and are also particularly concerned about the Whois situation in the so-called ccTLDs, the country code top-level domains, where in some instances there is precious little Whois information to be had and there's tremendous variability across all of those domains.

They were originally intended for use by the countries to whom they were issued; however, as you know, they can end up on the open market, in the case of dot-tv or dot-cc, for example, where they function precisely like generic top-level domains available to anyone to register space, but without that integral Whois capability that we depend on in finding a responsible party.

Mr. COBLE. I thank the gentleman. We've been joined by the lady from California, and I have a couple more questions, so I think the best thing for us to do is to break for the vote, and then we will

return. So you all rest easy, and we will be back imminently, probably—there are two votes. We'll probably be back in 15 to 20 minutes.

[Recess.]

Mr. COBLE. There was only one vote in lieu of the scheduled two, so we're back a little earlier. I guess Ms. Lofgren will come back. Let me start to question while we're waiting on her.

Messrs. Mitchell and Trainer, let me come back to you all. You all described some of the differences in the type of Whois structure among the various domains and country codes. Comment, if you will, briefly, on what features would go into a model Whois Database.

Mr. TRAINER. I know that Steve has responded eloquently to a couple of these questions. I'll try to provide a response on this one.

From an enforcement perspective, clearly, intellectual property owners always want as much as they can get. But given the fact that the information that we find oftentimes on the Whois Database or certainly our members find is false information. The name and address and other contact information, such as even an e-mail address or a phone number or something beyond just even the name and address, would certainly be helpful.

I think that intellectual property owners who are going after pirates and counterfeiters who don't follow rules at all because they are violating somebody else's rights, as much information as possible is always good. But I think that certainly the very basic things, the name, the address, an e-mail address, phone number, basic contact information is really what we're looking for in order to expedite the contact and try and resolve a problem.

I don't think that our members are looking for anything and everything. They're just looking for reasonableness in the ability to contact people whom they believe are violating copyrights and trademarks that they own. Thank you.

Mr. MITCHELL. Thank you, Mr. Chairman. We do believe that ICANN is on the right track with respect to the data that it demands in its registrar accreditation agreement. And we would point you back to section 3.3 of that agreement for the information that is currently required of the generic top-level domains, including the registered name, name server information, the identity of the registrar, name, postal address, e-mail address, voice telephone number, and fax number of the technical contact for the registered domain, as well as the administrative contact for the registered domain.

We would not be asking to expand this information dramatically, though, as I've mentioned, improvements could be made. We would, however, like to draw a distinction between the information for the technical contact, the person with their finger on the switch and the ability to terminate access to infringing material, and the identifying information of the registrant, the person who actually holds out themselves as the owner of the domain. We think both of those are necessary data elements, because in these situations, enforcement is not just about terminating access to the infringing material. It's about launching an investigation into the parties responsible.

Mr. COBLE. Thank you, sir.

Dr. Catlett, I was going to talk to you about special procedures, but I think you and Mr. Berman pretty well plowed that field. So let me direct attention to Ms. Fena.

Ms. Fena, let me put another two-part question to you. It's been suggested by some that we need to cut back on access to Whois in order to protect the "right of anonymity" on the Net. My two questions: Is there a legitimate role for anonymity online and is it consistent with the status quo regarding Whois, A? And, B, if you wish to be anonymous online, why can't one forego a domain name and use a numerical Internet protocol address?

Ms. FENA. I actually find that this question is probably one that would split any cocktail party down the middle. Whenever you get to the question of is there a right to anonymity and should there be a right to anonymity online, there are two important areas to address here. One, I think there is and should be, especially with the U.S. principles of free speech and the ability to have political speech and whistle-blowing capabilities in this online world, I think the right to anonymity is extremely important. However, I think that that right should be balanced, and in the case of the Whois Database, I don't think there is necessarily a right to an anonymous website address. And there may be other ways through proxy servers that would allow a certain amount of shielding or other ways to conduct private—or not private, but conduct speech.

We were actually just talking during the intermission about many community websites where it's actually people that are speaking on a community or have a small sub-site within a geocities site, and do you necessarily need to know the registrant information for somebody that has this incredibly long appended name. And I think that in the area of personal sites and community-type sites, it would be extremely important, and there probably are other ways to be anonymous.

I think it's extremely important in the Whois Database for the areas of both accountability not just for the intellectual property right owners but also for consumers as they're moving around on the Web to know who they're dealing with and have an ability to not have to go through a court process or get a subpoena to be able to access that kind of information. Especially in the Internet world, speed and ability to quickly access is extremely important.

So, yes, there should be a right to some anonymity and anonymous speech on the Internet. I don't think that we have to apply that completely within the Whois Database. There are abilities to use proxies and proxy kinds of services so that if somebody doesn't wish to register directly but have a third party sort of filter things for them, I think that kind of service is already available, but just not implemented today. I think that we should look at implementing that.

And two other areas that I think can improve that is the ability to have some attestation by the register—by the person registering that they are providing accurate information so we can use existing fraud laws to go after fraudulent behavior and information.

And, thirdly, limiting the use so that there is—it's different to—you shouldn't require everybody who registers for a domain that they are naturally also registering for junk mail. So having a provi-

sion to limit the use of the information so it's not available for automatic resell.

Thank you.

Mr. COBLE. Thank you.

Mr. Berman, second round.

Mr. BERMAN. Mr. Trainer, in your testimony you express frustration that ICANN doesn't enforce its provisions in its registrar contracts requiring registrars to verify Whois contact information. And you also note from your own experience that registrars do very little to verify or update Whois information.

If ICANN and registrars continue to be so lax, despite their contractual obligations, should Congress step in and require the Whois information be accurate and verified?

Mr. TRAINER. Well, I think that there may be an interim step, and that is, if ICANN were really put on notice by this Committee or another committee that there would be a period during which they would have to bring these agreements into proper compliance and implementation of the provisions of the agreement to see really how that works, to give them a chance perhaps to really implement what they already have with the registrars, and then between the registrars and the particular domain name registrants to see if, in fact, they're going to follow through, verify, and so on, certainly we may not need to go to the point of introducing law. But I do think the importance of ensuring that ICANN's accreditation agreements are actually being implemented and enforced is important.

What's interesting to us is just the IACC alone—unfortunately for us, we've moved a couple of times in the last couple of years. And checking our own domain name registration and in preparation for this hearing, we actually updated our address information. We have never been contacted by anyone to do that. And, in fact, I was surprised—I've only been at the IACC for 2 years, but the address that actually appeared was not our immediately previous address but the one before that. So we had actually moved twice in the last 2 years or so, but we've never been contacted by anyone as to a question is your information updated or any act by a registrar, Internet service provider or anybody, as far as making sure that we are actually in compliance. So—and we have absolutely no reason not to be in compliance. We want people to find us.

So it's interesting to us that our own experience would show that what we really need to see is whether ICANN can get the registrars to implement effectively their agreements.

Mr. BERMAN. Amen. Mr. Chairman, it's an interesting idea. In other words, sort of let them know that Congress has some expectations here, leaving pregnant the possibility of—

Mr. TRAINER. Actually, I think in our conclusory remarks, that's exactly what we were suggesting, is that ICANN truly be put on notice that we're watching, and you're watching, and that if things do not improve in the very short term, that other steps may be taken.

Mr. BERMAN. A follow-up question for Dr. Catlett. In your testimony, you note that the Whois information is rarely used—in use against career spammers.

Mr. CATLETT. Used by career spammers. Is rarely—

Mr. BERMAN. Is rarely of use against career spammers, yes, who have registered large numbers of domains with contact addresses such as the Martian Embassy.

Mr. CATLETT. Yes.

Mr. BERMAN. Wouldn't requirement and verification of accurate Whois information cure this deficiency and, therefore, make the Whois Database vastly more useful against career spammers?

Mr. CATLETT. I think if we examine a procedure that a registrar could reasonably require to go through, the answer is likely to be no. You can certainly have online services that will check that the Martian Embassy is not an accurate, correct address within the United States. But spammers would very quickly find out that such procedures were being applied, and they would register their domains instead as Lori Fena of a certain address, accurate address, in California, effectively stealing someone's identity in order to obtain a domain name—

Mr. BERMAN. Actually, accurate verification includes not just taking a real address on this Earth, this planet, but that the person is, in fact—that is the person's address.

Mr. CATLETT. So perhaps one could then add on an additional step, which would be to send a letter to the address saying, Congratulations, you've registered for the domain name evilcentral.com. But—and then what do you do? Do you take non-response to that as a verification? Do you require that they send that back in? I think that that's imposing an impractical burden. I mean, we've already heard testimony from one of the trade organizations that they were in violation of their obligation to maintain accurate information about their present address. And I think if that were universally applied, it would be impractical. And I think—also think it's inappropriate given the purpose of the Internet, which is a communications medium.

Mr. BERMAN. But if the spammer took Ms. Fena's name, may be involved in ID theft, they're guilty of a crime—

Mr. CATLETT. They're already involved a great deal.

Mr. BERMAN [continuing]. And they could be prosecuted. That might be some deterrent.

Mr. CATLETT. Well, they're already involved in a great deal of criminal activity. Spammers typically are committing fraud. So I don't think the prospect of also being involved in identity theft is going to be of much bother to them. They already, for example, give as return addresses other businesses who are then burdened with the task of explaining to angry consumers that they are not the person that's spammed them.

So I don't see as practical a method of trying to get absolute identification from anyone who registers for a domain name. Nor do I think it's appropriate given the way that the courts have regarded free speech and anonymity on the Internet to demand this kind of absolute identification as a condition.

We've heard from most of the witnesses that they regard the Internet as primarily a vehicle for commerce, and it certainly is important for that. But many people now are using it as a means of civil discourse. And I don't think that we should impose conditions appropriate for business on individuals as a precondition for that participation.

Mr. BERMAN. Well, my time, at least in this round, is expired. One last question. I want to understand that, notwithstanding what I said in my opening statement, why is there a right to anonymity? I mean, why—in e-mail, analogous to correspondence, getting a website, I mean, we run for elected office. We waive a lot of rights to privacy in that context, and we make a conscious decision. To the extent that people understand the situation, why isn't getting a website a recognition that, because of accountability, because of potentials for consumer fraud, because of potentials for theft, any more than somebody who gets up on a soapbox at Hyde Park has a right not to have his picture taken. Make the case a little more for why there should be protection for going this extra step? People could convey their messages in a lot of different ways without getting a website.

Mr. CATLETT. Yes. Why is there a right to anonymity? I think historically, if we look at the reason for the foundation of the United States, Thomas Paine wrote a book called—a pamphlet called “Common Sense.” He authored it anonymously, and he continued to author other publications, and I think that was one of the considerations of the Founders to encourage that kind of speech.

Now, on the Internet we could say, well, this is primarily a commercial medium, but it's not. Courts have remarked that the Internet is one of the greatest media for free speech——

Mr. BERMAN. Well, I'm not talking about the Internet. I'm talking about getting a domain name and a website.

Mr. CATLETT. Well, establishing a domain name is like making a little homestead on the Internet. It's the vehicle by which you can maintain a pseudonym——

Mr. BERMAN. And then I go down to the county recorder's office, and I can see what the property is worth and exactly who owns it and look at the deed and a whole bunch of accessible pieces of information about me come up when I want to get my little homestead.

Mr. CATLETT. Absolutely, and there are good reasons for that, such as——

Mr. BERMAN. Yes.

Mr. CATLETT [continuing]. Accountability for taxation, for example, and for the fact that a property owner can——

Mr. BERMAN. Maybe we should tax the Internet. No. [Laughter.]

Mr. COBLE. The gentleman's time has expired. [Laughter.]

Mr. COBLE. I thank the gentleman.

Ms. Lofgren, the gentlelady from California, I don't believe will be returning since she is not here.

Speaking of anonymity, you all may appreciate this. I was the recipient the other day of an e-mail that was—the content was libelous. It was a nasty, nasty—blasting me every way from every corner of the paper, and his concluding remark was that, “Because I fear you may come after me, I'm not going to identify myself.” But his name and address appeared at the outset.

I'm not the smartest guy in town, but I think I can match wits with this guy. He is not anonymous.

We thank you, panelists, for being with us, and thank those in the audience for the interest that you have shown. This is as How-

ard and I have said, by implication, anyway, this will not be the final installment on this matter.

This concludes the oversight hearing on the Whois Database, privacy and intellectual property issues. The record will remain open for 1 week.

Thank you again for your cooperation, and the Subcommittee stands adjourned.

Mr. BERMAN. I was just joking about taxing the Internet.

Mr. COBLE. Very good. I'm glad you said that.

[Whereupon, at 12:32 p.m., the Subcommittee was adjourned.]

APPENDIX

STATEMENTS SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE HOWARD COBLE, A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF NORTH CAROLINA

Good morning. The Subcommittee will come to order.

Today, the Subcommittee will continue its review of the Internet and domain name policies. The "Whois Database" is the popular name for a combination of information directories. The policies controlling the access and use of this information imply many things, including privacy issues, the ability to enforce intellectual property rights, empowering parents and consumers, aiding law enforcement in public safety activities, and important First Amendment rights.

Some observers have declared that the Internet bubble has burst and have administered last rites to the technology. Still, in many ways, the Internet is thriving and soon will expand even further. Every day more people are going on the Internet. New business models are being launched. Later this year, a variety of new generic Top Level Domains will go online which will encourage new and more diverse activities.

Despite the many positive aspects of the Internet, I am disappointed by the fact that there are continuing reports of consumer fraud, intellectual property violations (such as cybersquatting), and threats to privacy that occur online. There is a temptation to write more laws in response to the threats. However, I am told that our current legal framework may be adequate to protect the public—as long as the public knows who is the true operator or source behind a given web-site. It is my hope that as the Internet grows and these policies develop, the public can count on the availability of a robust and dynamic Whois Database.

Today we are fortunate to hear from a variety of experts across a variety of disciplines that will help us to understand the state of the Whois Database and what it means for copyright owners, trademark holders, privacy organizations; and, in turn, what the Internet means for small businesses, families across America, and the public.

It is my hope that they will deliver positive news. Yet, I want to assure everyone that this is not the final chapter of the Subcommittee's work overseeing Internet and domain issues. Finally, while I am reluctant to consider introducing legislation—that may be necessary should developments concerning the deployment, content, or access to the Whois Database prove unsatisfactory. As I have stated previously, the Subcommittee has a responsibility to the public—including all of the people who care about privacy, consumer protection, and intellectual property—to guarantee that the Internet develops as a legitimate medium for a range of exciting purposes and not as a bazaar for pirates and snake-oil salesmen.

I now turn to the Ranking Member, Mr. Berman, for his opening statement.

PREPARED STATEMENT OF THE HONORABLE HOWARD L. BERMAN, A REPRESENTATIVE
IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman,

Thank you for calling this hearing on the privacy and intellectual property issues raised by the public accessibility of the Whois database. This is clearly a complex set of issues, and I am glad that we are going to get a chance to explore them today.

The main questions involved with the Whois database—the list of who owns which website and how to contact them—are what information should be available and to whom should it be available. Policy decisions about the accessibility of Whois information must be made in light of the fact that new domains are now being cre-

ated. The Internet Corporation for Assigned Names and Numbers (ICANN) and ICANN-approved registries are creating new domains, which will exponentially increase the number of copyright and trademark infringing, cybersquatting, and defrauding web sites. If new problems like these are going to be created, then mechanisms for addressing these problems should also be created. One such mechanism is access to the Whois database, and accurate info therein, so that IP owners, fraud busters, and the police can track down those taking advantage of these newly created opportunities to break the law. Registries cannot create new problems and then not provide the means to address them.

When I said “complex” earlier, I was referring to the fact that, while the Whois database is a crucial and necessary tool used by law enforcement, by owners of intellectual property, and by consumers themselves, this tool can be misused by those who wish to send batches of unsolicited commercial e-mails or commit crimes such as stalking. Where to draw the line between what is necessary for a Whois directory and what is an invasion of privacy is a difficult question in many cases.

On either end of the spectrum, I believe that this line-drawing is easy. For web sites conducting e-commerce, why should they have a privacy right to keep their place of business and controlling owner a secret? A brick and mortar business must get a permit—a permit that is public information—to do business in a city. A business applying for a bulk mailing permit from the U.S. Postal Service must likewise disclose who they are and where they can be found—again, public information under the Freedom of Information Act. It seems eminently clear to me that websites conducting e-commerce have little “right to privacy.”

At the other end of the spectrum, however, a person who has a website for purely personal reasons, pictures of his cat, perhaps, or political complaints against a Member of Congress—shouldn’t that person be able to do his personal business without everyone knowing who he is and how he can be found? And isn’t political speech worth protecting by redacting the personally identifiable contact information for the website owner? Realistically, however, few websites will meet this “ideal” of a truly personal endeavor. Furthermore, it is virtually impossible for a registrar to pre-determine which sites are purely personal, and thus impossible to determine which registrants should be allowed to remain anonymous.

The problem comes in the fact that many websites do not fall at one end of the spectrum. Many businesses are run out of people’s homes, for example, and “personal websites” could have a page on which the owner has illegal digital copies of movies for sale. This latter instance is one that very much concerns me. We are going to hear today about the various ways in which owners of trademarks, patents and copyrights police their intellectual property over the Internet. Intellectual property owners are concerned about combatting both copyright and trademark infringements on the Internet, and cybersquatting is common enough that being able to find the person behind the site is clearly of extreme importance.

For many IP owners, the Whois database represents their only line of defense against infringement of their property, and for that reason it is critically important that the information that is in the Whois database be accurate and verifiable. When I ran my own search earlier this year, I found fraudulent Whois information—a Mr. Angel listed at 1234 Evil Avenue in a city where there is no Evil Avenue, let alone a 1234 Evil Avenue. We may find disagreement about what information should be publicly available, but I strongly believe that what information is there should be accurate.

Earlier this month, the Internet Corporation for Assigned Names and Numbers announced that it has launched a study to gauge the privacy concerns raised by the public accessibility of the whois database. This study is directed to anyone who has ever used the service, both in the global top level domains and in the 244 country-code top level domains. I look forward to seeing the results of this study, and comparing them to what we hear today from our witnesses.

Mr. Chairman, I’d like to thank you again for calling this hearing. I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE
IN CONGRESS FROM THE STATE OF MICHIGAN

As we all know the Who-Is database is an electronic and publicly- available list that Internet domain name registrars keep of the names and addresses of those operating each website. This hearing asks how much openness on the Internet is desirable. Openness can be good because it lets people know who they’re dealing with, but it also can subject people to harassment, and this complexity begs us not to act hastily.

Because the database is accessible on the Internet, it's a valuable tool for intellectual property owners to find the identity of someone illegally selling patented, trademarked, or copyrighted items on a website. That's a laudable use, but more individuals and families are setting up websites for non-commercial reasons, such as posting pictures, and do not want their addresses and phone numbers out there for all the world to see.

This anonymity is useful because marketers lift names from Who-Is and bombard site owners with mail and phone solicitations; clearly, this can be a huge nuisance. This seems like a good reason to let owners of non-commercial sites remain anonymous, but the solution isn't that simple: individuals also can infringe others' rights and shouldn't be able to cloak their illegal conduct in the guise of privacy.

And First Amendment issues are not far behind. For instance, I'm not certain that a political dissident operating a website simply for speech against the government should have to be identified on Who-Is. That type of disclosure probably wouldn't further any useful purpose but could subject people to persecution and harassment.

The breadth of these issues indicates that Congress should not act too quickly. We are dealing simultaneously with intellectual property rights, privacy rights, and free speech rights and cannot simply play a legislative game of Rochambeau to figure which one should win in the end.

MATERIAL SUBMITTED FOR THE HEARING RECORD

POWELL, GOLDSTEIN, FRAZER & MURPHY LLP

ATTORNEYS AT LAW

www.pgfm.com

PLEASE RESPOND: Washington Address

Sixteenth Floor
191 Peachtree Street, N.E.
Atlanta, Georgia 30303
404 572-6900
Facsimile 404 572-8909

Sixth Floor
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202 347-0006
Facsimile 202 624-7222

Direct Dial: 202-624-7228
E-mail: dquam@pgfm.com

July 19, 2001

The Honorable Howard Coble
Chairman, Courts, the Internet, and Intellectual Property
B-351A RHOB
Washington, D.C. 20515
Attn: Chris Katopis

Dear Chairman Coble:

On behalf of the International AntiCounterfeiting Coalition (IACC), I would like to reply to a question you posed during the July 12, 2001 hearing on the WHOIS database. Specifically, you asked for information regarding the monetary damages caused by counterfeiters and pirates over the Internet. While we do not have numbers for all industries, the following anecdotal information should be helpful in outlining the scope of the problem.

Several IACC members brought suit against an individual who owned and operated the site "www.Fakegifts.com." The companies used the WHOIS information available for the site to send Cease and Desist letters to the reported owner citing the infringement of their trademarks. The C&D letters were returned because the information contained in the WHOIS database was incorrect. The companies then hired private investigators to locate and serve the owner of the site and eventually secured a default judgment against the owner. The court awarded the trademark holders \$16 million in statutory damages for the willful infringement of their marks.

The court in the Fakegifts.com case awarded the maximum in statutory damages because the activities of the counterfeiter were so brazen. As indicated in the attached CNNfn article, the owner of Fakegifts.com stated that he works to avoid detection on the Internet by serving as his own Internet-service-provider. "They can't serve me if they can't find me. And even if they do shut down one site, I'll put up another." ("Net sees more bogus goods," CNNfn, December 14, 1999.) The owner went on to state, "I'm very much aware of what I'm doing, but the money is so good, I'm going to keep doing it."

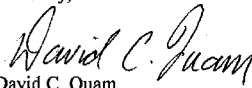
As the CNNfn article clearly demonstrates, counterfeiters and pirates know no rules other than quick and easy profits. The Internet only exacerbates the problem for intellectual property

POWELL, GOLDSTEIN, FRAZER & MURPHY LLP

owners and consumers by taking away the traditional warning signs of fraudulent goods such as location, physical inspection of the goods and personal contact with vendors. WHOIS database information is often the only identifying information an intellectual property owner or consumer has to provide them with some degree of transparency to an otherwise artificial world.

Thank you again for inviting the IACC to be a part of these important discussions.

Sincerely,



David C. Quam
Powell, Goldstein, Frazer & Murphy LLP
General Counsel for the International
AntiCounterfeiting Coalition

cc: Rep. Howard Berman
Tim Trainer

..ODMA\FCD\DOCS\WSH\228928\1

Net sees more bogus goods

Study finds increase in fake Rolex, Gucci, Mount Blanc products on Internet

By Staff Writer Rob Lenihan

December 14, 1999: 7:18 p.m. ET

NEW YORK (CNNfn) - "Psst, wanna buy a Rolex? Tell you where I'm gonna be ..."

As the holiday shopping season goes into hyper-drive, a new study finds that the number of luxury-goods Web sites selling bogus items is on the rise.

While some consumers think buying counterfeit products is a victimless crime, experts say buying fakes hurt legitimate businesses and can funnel money to shysters, organized criminals and even terrorist groups.

Cyveillance, an Arlington, Va.-based e-commerce intelligence company, said in its second annual Holiday Cyber Scams Study that 4 to 8 percent of the Web sites selling Gucci, Rolex and Mont Blanc-branded products are actually selling bogus items.

"The Internet is the street corner of the new millennium," said Brandy Thomas, Cyveillance's chairman and chief executive officer. "In the offline world, it's pretty much buyer beware. But on the Internet, you have access to 150 million users and instead of the shady guy on the street corner, you have a sophisticated-looking Web site."

Thomas said the impact of counterfeits or replicas on luxury-item makers can be staggering. He estimated that if online sales represent 5 percent of the \$150 billion luxury-goods market, losing even 2 percent of that translates into hundreds of millions in lost revenue.

"The Internet is the street corner of the new millennium."

---Brandy Thomas, CEO, Cyveillance

Thomas said the study, which analyzed more than 50,000 Web pages, focused on the blatant counterfeit sites that freely acknowledge they are selling knock-offs.

One such site, Fashionreplicas.com, sells "Gucci" handbags for \$49.95 and says it offers the fake items so that middle-income people will have a chance to buy luxury items they cannot afford.

This site links to fakegifts.com, which offers fake luxury watches, such as Rolex, Omega and Cartier, as well as knock-offs of Mont Blanc pens.

Brian Brokate, a partner in the law firm of Gibney, Anthony & Flaherty, general counsel for Rolex, said the company is suing the fakegifts site. He said Internet knock-offs have grown from being virtually non-existent three years ago to a problem that consumes 20 percent of Rolex's anti-piracy budget. A specific figure was not available.

Here are some tips from Cyveillance on fighting the fakes:

1. **Order from reputable sites with solid privacy policies.**
2. **If the price is too good to be true, guess what - it probably is.**
3. **Make sure the site has an adequate return policy and relies on a reputable shipping company.**
4. **On the ordering page, look for the prefix "https" indicating that you have entered a secure server area.**
5. **Check for a disclaimer near the order form indicating the site uses a Secure Socket Layer.**

Whenever the company discovers a site selling fake watches, which is nearly every day, Brokate said Rolex approaches the Internet-service provider and demands the offending site be taken down.

"The nice part about the Internet is that there's a whole layer of responsibility," he said.

"The Web-service providers are a layer you can appeal to."

Brokate said money from counterfeit purchases has ended up in the pockets of gangsters, money launderers, drug cartels, and even the terrorists behind the World Trade Center.

"These are not nice people who do this," he said.

Mark Voiers has a different view of the situation. As the owner of the California-based Replica.com and fakegifts.com, Voiers said in a telephone interview that he is merely giving a taste of the good life to people who normally would not have a chance at owning luxury items.

"I do not commit fraud," he said. "I am not defrauding the public. I buy these watches right down the street from Rolex's lawyers."

Voiers, who said he was also being sued by high-class pen maker Mont Blanc and others, said he was not taking business away from Rolex and, in fact, is helping the company, since he claims many people wear the fake Rolex while saving to buy the real thing.

"You can buy these things in any city in the world," he said. "I'm bringing it to the layman in Montana who doesn't have access to these big cities."

While his Web site is officially located in Los Angeles, Voiers, who sweeps his packages with a bug detector, declined to give his exact location.

"I'm my own Internet-service provider," he said. "They can't serve me if they can't find me. And even if they do shut down one site, I'll put up another."

Voiers said that his site, which has lasted one year, is the longest-running replica dealer on the Internet. And he said he has plans to put up six more sites next week.

"I'm very much aware of what I'm doing," he said, "but the money is so good, I'm going to keep doing it." [TOP](#)

Copyright © 2001, CNN America, INC.

ALL RIGHTS RESERVED

ELECTRONIC PRIVACY INFORMATION CENTER

TO WHOM IT MAY CONCERN: PLEASE ADVISE US OF ANY COMMENTS OR CONCERNS YOU MAY HAVE REGARDING THE INFORMATION CONTAINED HEREIN.

February 16, 2001

Representative Fred Upton
2333 Rayburn House Office Building
Washington, DC 20515

Representative Edward J. Markey
2108 Rayburn House Office Building
Washington, DC 20515

Senator Conrad Burns
187 Dirksen Senate Office Building
Washington, DC 20510

Senator Fritz Hollings
125 Russell Senate Office Building
Washington, DC 20510

Dear Congressmen,

We are writing to you on behalf of the Electronic Privacy Information Center (EPIC) to bring your attention to a privacy issue of importance to Internet users around the world, and of particular concern to users in the United States who register domain names. According to a report in *The Wall Street Journal* today, Network Solutions, Inc., the largest domain registration company in the country, is now selling information on 6 million Internet customers to direct marketers. The information was obtained by Network Solutions, Inc. for the purpose of registration and is not unlike motor vehicle information for which Congress has passed important privacy legislation, The Drivers Privacy Protection Act of 1994, that was recently upheld by the United States Supreme Court in *Reno v. Condon*, 528 U.S. 141.

We are writing to you to urge you to examine whether this sale is currently permissible and if so, whether it is therefore necessary to adopt new legislation to safeguard the information that is provided by Internet users and companies as a condition of registering a domain name. We believe that the sale violates well established principles of U.S. law as well as international privacy standards, including privacy rules specifically developed to address concerns related to privacy in the context of domain name registration.

Thus far privacy has received only passing attention during the discussion of ICANN's authority. The Subcommittee on Communications recently held hearings on the Internet Corporation for Assigned Names and Numbers, otherwise known as ICANN. ICANN is the central authority for all Internet users worldwide that wish to register a domain name. As mentioned during the recent hearings held by your Subcommittee, part of ICANN's responsibility is to protect the privacy of its domain name registrants. Also mentioned during the hearings was the low level of privacy protection offered for this personal information. As you pursue further work on ICANN, we urge you to focus on the much-needed privacy protections for this personal information.

A domain name is virtually required for any individual or organization that wishes to establish a website. Only once an individual or organization obtains a domain name can one participate fully in the Internet that has been recognized by federal courts as "the most participatory form of mass speech yet developed," *Reno v. ACLU*, 929 F. Supp. 824, 883 (E.D. Pa. 1996) aff'd 521 U.S. 844 (1997). However, before one can participate in this medium, domain name registrants are required to provide personal information for the purpose of billing and other technical reasons. The types of information required for registration include name, mailing address, email address, and telephone number.

There are three major privacy issues that must be addressed when considering the treatment of this information. The first is how the registrar, the company that processes the registration of a domain name, is permitted to use the information in its possession. The most direct guidance for the level of privacy protection a registrar must provide is the ICANN Registrar Accreditation Agreement (RAA) (<http://www.icann.org/nsi/icann-raa-04nov99.htm>). The RAA was approved by the ICANN Board of Directors in November 1999. At that time, Network Solutions, Inc. was the only registrar that could process domain name registrations for .com, .net, and .org, by far the most popular top-level domains (TLDs) in which individuals and

http://www.epic.org/privacy/Internet/ICANN_privacy.html

organization were registering domain names.

Part of the RAA specifically allows registrars to sell bulk access to their databases of domain name registrants for a fee (see RAA II.F.6). Further, registrars that choose to sell bulk access to their databases are only restricted to the extent that the third-party recipient of the data does not use registrant data to send unsolicited commercial email (also known as spam) and that they may establish an opt-out for registrants if they so wish. In addition, ICANN has sought to restrict the ability of registrars to establish a higher level of privacy protection on their own, see ICANN's Amicus Curiae Memorandum, *Register.com, Inc. v. Verio Inc.*, (<http://www.icann.org/registrar/register.com-verio/amicus-22sep00.htm>).

Such a permissive policy with respect to registrant data has led to attempts by registrars to aggressively market the personal data of domain name registrants. For example, the dotcom.com website, owned by VeriSign and its subsidiary Network Solutions Inc., displays the following message on its "Data Services" webpage at <http://www.dotcom.com/services/>:

Winning With Data From Network Solutions

Ready to win the Internet marketing game? Take your marketing program to the next level with Data Services from Verisign/Network Solutions. No other source offers the reach and depth of data when targeting companies who are doing business on the Internet.

Taking advantage of our position as a market leader, we have organized our pool of over 15 million registered domain names into a customer database of over 5 million unique customers. Our data service offers access to the key decision-makers behind millions of leading Web businesses.

We also track the progress of sites through key stages in the dotcom lifecycle, including live or not-live sites, e-commerce status, membership features and more. Want to target only small businesses with live sites? Nobody offers a better snapshot of this hard-to-reach group than we do. After all, over 80 percent of our customers are small businesses, representing every major small business category you could hope to reach.

For ISPs and other service providers, meanwhile, we offer extensive data on registered businesses' site switching behavior and hosting arrangements. ISPs and Web hosting firms can use this data to target customers when they're most likely to be ready for new opportunities.

To learn more about this unique service, just fill out the form below, and we'll follow up shortly. If you'd prefer, you may also get in touch via phone at (866) 293-5710.

The second privacy issue is how a registrar chooses to enter or make available such information in the Whois database. The Whois database is a publicly accessible database that allows *any* individual to look up information about a holder of a domain name. (You may want to examine the information available at www.allwhois.com or www.betterwhois.com.) For good reasons related to the technical and security considerations of maintaining websites and domains, it is necessary to make such information publicly available. Making such contact information available has been the practice of the domain name process for many years and is well-accepted by the many in the Internet community.

However, over the past few years, as the Internet has grown in enormous popularity, non-technically inclined individuals and families are registering domain names for personal use. Similarly, many entrepreneurs are taking advantage of the Internet to launch their businesses and may be operating out of their own homes. But, in both these cases, many people who register domain names are unaware that their home address and phone number will immediately become available to any Internet user in the world.

A third issue closely tied to the privacy concerns outlined above, but with First Amendment implications, is that the current level of privacy protections essentially eliminates the ability of Internet users to anonymously register domain names. Anonymous publication of information is well recognized in U.S. case law. In *McIntyre v. Ohio Elections Commission*, the U.S. Supreme Court stated that:

Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation; and their ideas from suppression; at the hand of an intolerant society. 514 U.S. 334, 357 (1995).

In short, a First Amendment right to anonymous publication is currently invalidated by the procedures adopted by ICANN, which some have argued is a government actor, with respect to domain name registration and the

http://www.epic.org/privacy/Internet/ICANN_privacy.html

July 9, 2001

Letter on Privacy of Domain Name Registration (02/16/01)

Whois database.

We urge the Subcommittee on Communications to closely examine these issues and consider them during future hearings on ICANN. In these upcoming hearings, we urge the members of the Subcommittee to explore how:

- (1) How well ICANN and ICANN-accredited registrars seek to limit the amount and types of information collected about domain name registrants and/or made available through the Whois database.
- (2) Efforts are made to educate domain name registrants about the existence and purpose of the Whois database.
- (3) ICANN and ICANN-accredited registrars can and should raise the level of privacy protection offered domain name registrants.
- (4) ICANN and ICANN-accredited registrars can and should prevent the sale of personal data collected from domain name registrants.
- (5) Ways in which ICANN and ICANN-accredited registrars can enable anonymous registration of domain names.
- (6) Whether ICANN, as a body with international reach, complies with data protection laws around the world that seek to protect personal information.
- (7) Whether legislation is necessary to safeguard the privacy interests of Americans who register an Internet domain name.

Privacy protection is critical to establish trust and confidence in network services. We believe that the recent decision by Network Solutions to sell data on Internet users provided simply for the purpose of domain name registration poses a substantial risk to the future growth of the Internet. We urge you to pursue this issue.

Sincerely yours,

/s/

Marc Rotenberg
Executive Director
EPIC

/s/

Andrew Shen
Policy Analyst
EPIC

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

July 12, 2001

U.S. House of Representatives Committee on the Judiciary
Subcommittee on Courts, the Internet and Intellectual Property
B351A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Coble, Representative Berman, and Members of the
Subcommittee,

We are writing to you on behalf of the Electronic Privacy Information Center (EPIC) to express our organization's views on the free speech and privacy issues implicated in the Whois database.¹ We appreciate the Subcommittee's decision to hold a hearing on this topic on July 12, 2001 and request that this statement be included in the hearing record.

EPIC is a public interest center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC staff has participated as counsel in landmark Internet free speech cases such as *Reno v. ACLU* and as advocates for stronger online privacy protection. We wish to highlight the expertise of EPIC in the areas of Internet free speech and privacy precisely because these are two of the most important interests affected by Whois database practices.

We have previously written on the privacy issues involved in domain name registration to both the House Subcommittee on Telecommunications and the Internet and the Senate Subcommittee on Communications. That letter addressed

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)
www.epic.org

¹ Network Solutions, Inc., the largest domain name registry and registrar, defines a domain name as: "[a]n addressing construct used for identifying and locating computers on the Internet. Domain names provide a system of easy-to-remember Internet addresses, which can be translated by the Domain Name System (DNS) into the numeric addresses (Internet Protocol (IP) numbers) used by the network. A domain name is hierarchical and often conveys information about the type of entity using the domain name" (<http://www.networksolutions.com/cgi-bin/glossary/lookup?term=Domain%20Name>). In order to establish an easy-to-find and easy-to-remember online presence, a person or organization must register a domain name. Additionally, a domain name often indicates something about the nature of the information contained on a particular website or the entity presenting that information.

the marketing of domain name registrant data by registrars, the Whois database, and the importance of anonymous speech.²

We now wish to express our opinion on how to go forward on the specific issue of the Whois database. Our primary concern is that the submission of identifying information for inclusion in the Whois database should be voluntary. We believe this is important to protect free speech and privacy interests.

Free speech and anonymity on the Internet

Fundamental to our view of the domain name issue is the importance of Internet free speech and the right of anonymity that has been recognized by the U.S. courts. The Supreme Court's unanimous decision in *Reno v. ACLU* offers an opinion on why individuals and organizations would want to display material through the World Wide Web:

Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.³

For the purposes of political, artistic or controversial speech, the Internet is an unprecedented opportunity to reach a large audience at a relatively small cost. The one-to-many characteristics of the Internet through which an individual's speech can reach a global audience are further enhanced by the protection of anonymity. In *McIntyre v. Ohio Elections Commission*, the Supreme Court upheld the ability to distribute anonymous political leaflets and found:

Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation; and their ideas from suppression; at the hand of an intolerant society.⁴

² "Letter on Privacy of Domain Name Registration (02/16/01)," http://www.epic.org/privacy/internet/ICANN_privacy.html.

³ *ACLU v. Reno*, 521 U.S. 844, 896-897 (1997).

⁴ *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995).

David L. Sobel, General Counsel at EPIC, has commented that "[t]he protection of anonymity . . . takes on added significance on the Internet, a medium which provides individuals with unprecedented opportunities to both publish and receive information."⁵

Current identification requirements of domain name registration

The requirements of the Whois database are most directly governed by the Internet Corporation for Assigned Names and Numbers (ICANN) Registrar Accreditation Agreement (RAA). That document requires registrars to provide public access to the identity and mailing address for the domain name holder and the identities, mailing addresses, email addresses, telephones and fax numbers for the technical and administrative contacts.⁶ It is not uncommon for the domain name holder to also be listed as the administrative contact; thus, the domain name holder will also often have her email address, telephone and fax number displayed to the general public.

The penalty for not providing this information is the loss of the registered domain name:

A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.⁷

Thus, if an Internet user refuses to provide contact information to a domain name registrar that will eventually be made publicly available to anyone with Internet access, she will also lose the ability to register a domain name. Current requirements are then placing a burden on the ability of individuals to maintain their anonymity and thus their

⁵ David L. Sobel, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, 5 Va. J.L. & Tech. 3 (2000), <<http://www.vjolt.net/vol5/symp2000/v5i1a3-Sobel.html>>.

⁶ See Section 3.3, ICANN Registrar Accreditation Agreement (17 May 2001), <<http://www.icann.org/registrars/ra-agreement-17may01.htm>>. To see a sample Whois record, see Revised VeriSign .com Registry Agreement: Appendix O (16 April 2001), <<http://www.icann.org/tlds/agreements/verisign/registry-agmt-appo-com-16apr01.htm>>.

⁷ Id. at Section 3.7.7.2.

fullest ability to exercise free speech online. Compelling the disclosure of personal information in such a manner could pose far-reaching dangers to Internet free speech.⁸

It should be noted that the ICANN RAA does provide a way for an individual to license the use of a domain name to a third party.⁹ The establishment of an intermediary between the operator of a website and the general public may avoid short-term identification of the actual user of a particular domain name. However, for the most controversial artistic, political and religious speech, it will be difficult for an online speaker to find an intermediary that will offer to have her own identity made public in lieu of the actual speaker. In addition, the third-party licensing provision is unambiguous in stating that the intermediary will be directly liable for use of the domain name by the actual user.

Other public policy reasons to encourage the provision of Whois data

Understandably, there are public policy reasons for identifying the holder of a domain name and making that information available to the general public. The Whois database is useful for contacting systems administrators about network or security problems. Some use Whois capabilities to find spammers or those who send unsolicited commercial e-mail. Accurate Whois information is also used for consumer protection purposes to identify who is managing a particular business operation. Whois data is also used for tracking intellectual property infringements and other infractions of the law. However, these reasons do not trump the strong free speech interests at play.¹⁰

⁸ The need for anonymous Internet activity, including the anonymous hosting of websites and domain name registration, is far from hypothetical. Different political, artistic and religious groups around the world rely on the Internet to avoid persecution - and anonymity will make this easier. See Lakshmi Chaudhry, "Virtual Refuge for Gay Muslims," *Wired News*, May 8, 2000, <<http://www.wired.com/news/print/0,1294,35896,00.html>>; Sarah Gauch, "Effects of Arab censorship blunted by Internet," *Christian Science Monitor*, January 29, 2001, <<http://archive.nandotimes.com/technology/story/0,1643,500304664-500488126-503379336-0,00.html>>; Anya Schiffrin, "Analysis: China, the Net and free speech," *The Industry Standard*, February 16, 2001, <<http://www.cnn.com/2001/TECH/internet/02/16/huang.qi.idg/index.html>>; Craig S. Smith, "Sect Clings to the Web in the Face of Beijing's Ban," *New York Times*, July 5, 2001, <<http://www.nytimes.com/2001/07/05/world/05FALU.html>>.

⁹ ICANN Registrar Accreditation Agreement (17 May 2001), Section 3.7.7.3.

¹⁰ Internet users may have further suggestions about the voluntary submission proposal. ICANN is currently conducting its own survey of the Internet community's attitudes towards the Whois database. Any member of the public can provide their views on proper Whois policies directly to that organization. See DNSO Names Council Whois Survey, <<http://www.icann.org/dnsso/whois-survey-en-10jun01.htm>>.

Registrars and others should continue to offer the Whois database as a service to the public but they should not condition the registration of a domain name on the display of personal information of the domain name holder. Requiring all individuals to display that information is a different matter than maintaining the Whois database on a voluntary submission basis.

At first, this may seem like a radical policy since it relies entirely on the domain name holder's discretion on whether to display accurate and complete contact information to the general public. But this is close to what is currently common practice. A significant amount of information currently submitted is not accurate and the vast majority is not verified by the registrar. In practice, it is up to the domain name holder to decide what information to submit to the registrar and consequently displayed to the public via the Whois database. This current practice does not significantly disrupt Internet activities and should be codified by changing the relevant ICANN documents.

Allowing individuals to decide whether to identify themselves also allows them to weigh the competing interests for displaying their contact information. In some instances, they may benefit due to the security alerts that arrive through Whois contact data. It would also be beneficial to domain name holders to display accurate information in order to respond in a timely manner to domain name disputes.

To further encourage the public to voluntarily submit Whois data, EPIC would suggest that registrars require less data for Whois records. For example, it may not be necessary to require fax numbers be provided for the administrative and technical contacts in addition to the e-mail, postal or telephone communications.

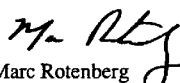
Conclusion

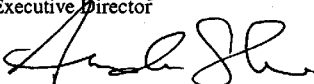
Maintaining anonymity on the Internet is difficult.¹¹ Providing anonymous registration of domain names as the default will not preserve Internet anonymity in all instances but it will offer some assistance to online publishers that have a need to hide their identities. Thus, in order to take full advantage of the Internet's unprecedented potential for encouraging the dissemination of speech, the Subcommittee should support the voluntary submission of domain name holder identifying information to the Whois database. We also believe that including less information in a Whois record will encourage the

¹¹ See, for a general description of the information trails left by Internet users, Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1220-1238 (1998), <<http://www.law.ucla.edu/Faculty/Bios/KANG/Scholarship/cprivacy.pdf>>.

voluntary submission of such information by lessening the privacy exposure that results.
We encourage the Subcommittee to urge ICANN to support this policy as well.

Sincerely,


Marc Rotenberg
Executive Director


Andrew Shen
Senior Policy Analyst

○